

PCT/JP00/09129

22.12.00

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

JP00/9129

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application:

2000年 1月14日

REC'D 02 MAR 2001

WIPO PCT

出願番号
Application Number:

特願2000-005161

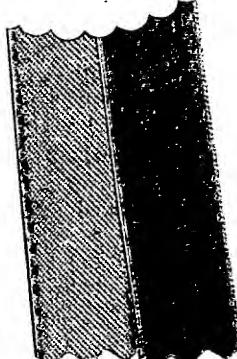
4

出願人
Applicant(s):

三菱電機株式会社

PRIORITY
DOCUMENT

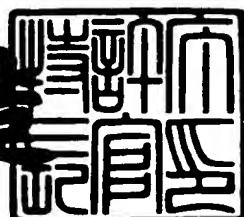
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)



2001年 2月 9日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3005395

【書類名】 特許願
【整理番号】 522196JP01
【提出日】 平成12年 1月14日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 9/06
【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

【氏名】 反町 亨

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

【氏名】 時田 俊雄

【特許出願人】

【識別番号】 000006013

【氏名又は名称】 三菱電機株式会社

【代理人】

【識別番号】 100099461

【弁理士】

【氏名又は名称】 溝井 章司

【選任した代理人】

【識別番号】 100111497

【弁理士】

【氏名又は名称】 波田 啓子

【選任した代理人】

【識別番号】 100111800

【弁理士】

【氏名又は名称】 竹内 三明

【手数料の表示】

【予納台帳番号】 056177

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9903016

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化装置及び暗号化方法及び復号装置及び復号方法

【特許請求の範囲】

【請求項1】 1つ以上のブロックデータからなる第1の処理データと、1つ以上のブロックデータからなる第2の処理データとの暗号化処理をする暗号化装置において、

暗号化処理の状態を記憶するメモリを備え、

第1の処理データの全ブロックデータの暗号化処理が完了する前に第2の処理データの最初のブロックデータの暗号化処理を開始するとともに、第2の処理データの最初のブロックデータの暗号化処理を開始する場合に第1の処理データの暗号化処理の状態を上記メモリに記憶させ、第1の処理データの暗号化処理を再開する場合に暗号化装置の暗号化処理の状態をメモリに記憶した第1の処理データの暗号化処理の状態に復帰させてから第1の処理データの暗号化処理を再開することを特徴とする暗号化装置。

【請求項2】 上記暗号化装置は、第2の処理データの全ブロックデータの暗号処理の完了する前に第1の処理データの暗号化処理を再開するとともに、上記メモリは、第1の処理データの暗号化処理を再開する場合に第2の処理データの暗号化処理状態を記憶し、第2の処理データの暗号化処理を再開する場合は、暗号化装置の暗号化処理の状態をメモリに記憶した第2の処理データの暗号化処理の状態に復帰させてから第2の処理データの暗号化処理を再開することを特徴とする請求項1記載の暗号化装置。

【請求項3】 上記第1の処理データは、第1の平文であり、上記第2の処理データは、第2の平文であることを特徴とする請求項1記載の暗号化装置。

【請求項4】 上記暗号化装置は、割り込みにより第2の処理データの最初のブロックデータの暗号化処理を開始することを特徴とする請求項1記載の暗号化装置。

【請求項5】 平文Mを構成する平文ブロックデータM_i (i = 1, 2, 3, ...) と平文Nを構成する平文ブロックデータN_j (j = 1, 2, 3, ...) とを暗号化する暗号化装置において、

平文Mの暗号化処理中に平文Nの暗号化要求を平文Mの暗号化処理完了前に受け付けるメカニズムと、

暗号化処理を行い中間ブロックデータ T_i 又は暗号文ブロックデータ C_i を出力する暗号化モジュールと、

暗号化モジュールから出力された中間ブロックデータ T_i 又は暗号文ブロックデータ C_i をフィードバックラインを介し暗号化モジュールにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記平文Nの暗号化要求を受け付け、平文Nのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されない場合、フィードバックされるブロックデータを記憶するメモリと、

平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化される場合は、上記フィードバックループのフィードバックラインによりフィードバックされるブロックデータを選択してフィードバックループに供給し、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されず、平文Nのいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリに記憶されたブロックデータを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする暗号化装置。

【請求項6】 上記メモリは、

複数の平文に対応した複数のレジスタと、

暗号化処理をする平文に対応してレジスタを切り替えるスイッチと
を備えたことを特徴とする請求項5記載の暗号化装置。

【請求項7】 暗号化モジュールを用いて第1の平文Mの平文ブロックデータ M_i ($i = 1, 2, 3, \dots$) を暗号化する工程と、

上記平文ブロックデータ M_i を暗号化している途中で又は平文ブロックデータ M_i を暗号化した後に、第1の平文Mの平文ブロックデータ M_{i+1} の暗号化に用いられる中間ブロックデータ T_i 又は暗号文ブロックデータ C_i をメモリに記憶

する工程と、

上記平文ブロックデータ M_{i+1} の暗号化に用いられるブロックデータをメモリに記憶した後に、第2の平文Nの少なくとも1つの平文ブロックデータを暗号化する工程と、

上記第2の平文Nの少なくとも1つの平文ブロックデータを暗号化した後に、メモリに記憶された、平文ブロックデータ M_{i+1} の暗号化に用いられるブロックデータを入力し、暗号化モジュールを用いて第1の平文Mの平文ブロックデータ M_{i+1} を暗号化する工程と

を備えたことを特徴とする暗号化方法。

【請求項8】 1つ以上の平文ブロックデータからなる平文を暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、

平文ブロックデータを暗号化したときに生成した中間ブロックデータ T_i 又は暗号文ブロックデータ C_i をフィードバックする第1のフィードバックループを有し、平文ブロックデータを入力し、第1のフィードバックループによりブロックデータをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化部と、

認証子演算途中結果をフィードバックする第2のフィードバックループを有し、暗号化部から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第2のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成部と

を備えたことを特徴とする暗号化装置。

【請求項9】 上記暗号化部と認証子生成部とは、1つの暗号化モジュールと、1つのフィードバックループとを兼用して暗号化処理と認証子生成処理とを交互に行うとともに、

上記1つのフィードバックループは、

暗号化処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

暗号化処理と認証生成処理とを交互に実行するために、メモリから暗号化処理

と認証子生成処理との結果を交互に選択して暗号化モジュールに出力するセレクタと

を備えたことを特徴とする請求項8記載の暗号化装置。

【請求項10】 1つ以上の平文ブロックデータからなる平文を暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化方法において、

平文ブロックデータを暗号化したときに生成した中間ブロックデータ T_i 又は暗号文ブロックデータ C_i をフィードバックする第1のフィードバック工程を有し、平文ブロックデータを入力し、第1のフィードバックループによりブロックデータをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化工程と、

認証子演算途中結果をフィードバックする第2のフィードバック工程を有し、暗号化工程から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第2のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成工程と

を備えたことを特徴とする暗号化方法。

【請求項11】 1つ以上のブロックデータからなる第1の処理データと、1つ以上のブロックデータからなる第2の処理データとの復号処理をする復号装置において、

復号処理の状態を記憶するメモリを備え、

第1の処理データの全ブロックデータの復号処理が完了する前に第2の処理データの最初のブロックデータの復号処理を開始するとともに、第2の処理データの最初のブロックデータの復号処理を開始する場合に第1の処理データの復号処理の状態を上記メモリに記憶させ、第1の処理データの復号処理を再開する場合に復号装置の復号処理の状態をメモリに記憶した第1の処理データの復号処理の状態に復帰させてから第1の処理データの復号処理を再開することを特徴とする復号装置。

【請求項12】 上記復号装置は、第2の処理データの全ブロックデータの

復号処理の完了する前に第1の処理データの復号処理を再開するとともに、上記メモリは、第1の処理データの復号処理を再開する場合に第2の処理データの復号処理状態を記憶し、第2の処理データの復号処理を再開する場合は、復号装置の復号処理の状態をメモリに記憶した第2の処理データの復号処理の状態に復帰させてから第2の処理データの復号処理を再開することを特徴とする請求項11記載の復号装置。

【請求項13】 上記第1の処理データは、第1の暗号文であり、上記第2の処理データは、第2の暗号文であることを特徴とする請求項11記載の復号装置。

【請求項14】 上記復号装置は、割り込みにより第2の処理データの最初のブロックデータの復号処理を開始することを特徴とする請求項11記載の復号装置。

【請求項15】 暗号文Cを構成する暗号文ブロックデータC_i (i = 1, 2, 3, ...)と暗号文Nを構成する暗号文ブロックデータN_j (j = 1, 2, 3, ...)とを復号する復号装置において、

暗号文Cの復号処理中に暗号文Nの復号要求を任意の時点で受け付けるメカニズムと、

復号処理を行い中間ブロックデータT_i 又は平文ブロックデータM_i を出力する復号モジュールと、

復号モジュールから出力された中間ブロックデータT_i 又は平文ブロックデータM_i をフィードバックラインを介し復号モジュールにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記暗号文Nの復号要求を受け付け、暗号文Nのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータC_{i+1} が暗号文ブロックデータC_i の次に続けて復号されない場合、フィードバックされるブロックデータを記憶するメモリと、

暗号文ブロックデータC_{i+1} が暗号文ブロックデータC_i の次に続けて復号される場合は、上記フィードバックループのフィードバックラインによりフィード

バックされるブロックデータを選択してフィードバックループに供給し、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されず、暗号文Nのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリに記憶されたブロックデータを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする復号装置。

【請求項16】 上記メモリは、

複数の暗号文に対応した複数のレジスタと、

復号処理をする暗号文に対応してレジスタを切り替えるスイッチと
を備えたことを特徴とする請求項11記載の復号装置。

【請求項17】 復号モジュールを用いて第1の暗号文Cの暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$) を復号する工程と、

上記暗号文ブロックデータ C_i を復号している途中で又は暗号文ブロックデータ C_i を復号した後に、第1の暗号文Cの暗号文ブロックデータ C_{i+1} の復号に用いられる中間ブロックデータ T_i 又は平文ブロックデータ M_i をメモリに記憶する工程と、

上記暗号文ブロックデータ C_{i+1} の復号に用いられるブロックデータをメモリに記憶した後に、第2の暗号文Nの少なくとも1つの暗号文ブロックデータを復号する工程と、

上記第2の暗号文Nの少なくとも1つの暗号文ブロックデータを復号した後に、メモリに記憶された、暗号文ブロックデータ C_{i+1} の復号に用いられるブロックデータを入力し、復号モジュールを用いて第1の暗号文Cの暗号文ブロックデータ C_{i+1} を復号する工程と

を備えたことを特徴とする復号方法。

【請求項18】 1つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、

暗号文ブロックデータを復号したときに生成した中間ブロックデータ T_i 又は平文ブロックデータ M_i をフィードバックする第1のフィードバックループを有

し、暗号文ブロックデータを入力し、第1のフィードバックループによりブロックデータをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号部と、

認証子演算途中結果をフィードバックする第2のフィードバックループを有し、復号部に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第2のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成部と
を備えたことを特徴とする復号装置。

【請求項19】 上記復号部と認証子生成部とは、1つの復号モジュールと、1つのフィードバックループとを兼用して復号処理と認証子生成処理とを交互に行うとともに、

上記1つのフィードバックループは、
復号処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、
復号処理と認証生成処理とを交互に実行するために、メモリから復号処理と認証子生成処理との結果を交互に選択して復号モジュールに出力するセレクタと
を備えたことを特徴とする請求項18記載の復号装置。

【請求項20】 1つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号方法において、

暗号文ブロックデータを復号したときに生成した中間ブロックデータ T_i 又は平文ブロックデータ M_i をフィードバックする第1のフィードバック工程を有し、暗号文ブロックデータを入力し、第1のフィードバックループによりブロックデータをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号工程と、

認証子演算途中結果をフィードバックする第2のフィードバック工程を有し、復号工程に入力される暗号文のブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第2のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認す

るための認証子を生成する認証子生成工程と
を備えたことを特徴とする復号方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、暗号化復号装置及び暗号化復号方法に関するものである。特に、データの暗号化復号の最中に他のデータの暗号化復号ができる発明に関するものである。

【0002】

【従来の技術】

図32は、Cipher Block Chaining Mode（以下、CBCモードという）による暗号化装置を示す図である。

図32に示すCBCモードでの暗号方法は、64ビットの平文ブロックデータ M_i をブロック単位で入力して、暗号鍵Kを用いた暗号化モジュール51により暗号化し、更に、この暗号化された暗号文ブロックデータ C_i と次の平文ブロックデータ M_{i+1} との排他的論理和を演算し、排他的論理和の演算結果を次の暗号化の入力として、暗号鍵Kを用いた暗号化モジュール51に供給することにより暗号化する方法である。そして、この処理を繰り返して次々と連鎖させることにより、平文M全体を暗号文Cに暗号化するものである。

【0003】

図33は、CBCモードを用いた復号装置を示す図である。

図33に示す復号装置は、図32に示す暗号化装置により暗号化された暗号文を復号する装置である。暗号文ブロックデータ C_1 が暗号鍵Kを用いた復号モジュール71に入力され、イニシャルバリューIVとの排他的論理和が計算され、平文ブロックデータ M_1 が復号される。暗号文ブロックデータ C_2 が入力された場合には、暗号鍵Kを用いた復号モジュール71で復号され、先に入力され、レジスタ111に保存された暗号文ブロックデータ C_1 との排他的論理和がとられ、平文ブロックデータ M_2 を復号する。

【0004】

平文ブロックデータを M_i ($i = 1, 2, \dots, n$)、暗号文ブロックデータ C_i ($i = 1, 2, \dots, n$) とし、暗号鍵 K を用いた暗号化処理を E_K 、暗号鍵 K を用いた復号処理を D_K とすると、CBCモードは次式で表される。

$$C_1 = E_K(M_1 \text{ EXR } IV)$$

$$C_i = E_K(M_i \text{ EXR } C_{i-1}) \quad (i = 2, 3, \dots, n)$$

$$M_1 = D_K(C_1) \text{ EXR } IV$$

$$M_i = D_K(C_i) \text{ EXR } C_{i-1} \quad (i = 2, 3, \dots, n)$$

ここで、EXRは排他的論理和演算である。また、IV (Initial Value) は初期値であり、最初の暗号化と復号の際に用いられる。イニシャルバリュー IV は、暗号化側と復号側で同一の値を用いる。

【0005】

図34は、Output Feedback Mode (以下、OFBモードという) の暗号化装置を示す図である。

図35は、OFBモードの復号装置を示す図である。

図36は、Cipher Feedback Mode (以下、CFBモードという) の暗号化装置を示す図である。

図37は、CFBモードの復号装置を示す図である。

【0006】

図38は、CBCモードの暗号化装置を用いて平文Mと平文Nを暗号化する手順を示す図である。

ここでは、平文Mが平文ブロックデータ M_1 、平文ブロックデータ M_2 、平文ブロックデータ M_3 から構成されており、平文Nが平文ブロックデータ N_1 のみで構成されている場合を説明する。

平文ブロックデータ M_1 の暗号化がスタートすると、暗号文ブロックデータ C_1 が出力されるとともに、暗号文ブロックデータ C_1 は、平文ブロックデータ M_2 の暗号化に用いられる。このように、暗号文ブロックデータ C_i は、平文ブロックデータ M_{i+1} の暗号化にフィードバックされて連鎖処理が行われる。従って、平文ブロックデータ M_1 から平文ブロックデータ M_3 までの暗号化が終わらなければ、平文ブロックデータ N_1 の暗号化を行うことができない。

【0007】

図39は、図38と同様に、CBCモードで暗号化を行う場合を示している。

図39の場合は、平文ブロックデータ M_1 、平文ブロックデータ M_2 、平文ブロックデータ M_3 の各データが準備されるのに時間がかかるてしまう場合を示している。一方、暗号化処理は、次の平文ブロックデータ M_{i+1} が準備できる前に終了しており、アイドル時間（例えば、T1～T2、T3～T4の時間）が発生してしまう場合を示している。このように、アイドル時間が発生する場合でも、暗号文ブロックデータ C_i が次の平文ブロックデータ M_{i+1} にフィードバックされる連鎖処理を行わなければならないため、平文ブロックデータ N_1 の処理は平文ブロックデータ M_3 の処理が終了してからでなければ行えない。

【0008】

図40は、データの秘匿処理とデータの完全性を保証する処理を示す図である。平文Mは、例えば、OFBモードの暗号装置により暗号文Cに暗号化される。CBCモードの暗号装置により認証子Pが演算され、暗号文Cの最後に認証子Pが付加される。暗号化され、かつ、認証子Pが付加されたデータを受信した場合には、暗号文Cから平文MをOFBモードの復号装置により復号するとともに、暗号文CからCBCモードの復号装置により認証子Pを演算し、伝送されてきた認証子Pと同一か否かを比較することにより、伝送されてきたCが改竄されていないことを確認することができる。

【0009】

図41は、図40に示した秘匿処理と認証子演算処理の手順を示す図である。

平文ブロックデータ M_1 ～平文ブロックデータ M_3 は、順に暗号文ブロックデータ C_1 ～暗号文ブロックデータ C_3 に暗号化される。その後、暗号文ブロックデータ C_1 ～暗号文ブロックデータ C_3 を順に入力して認証子Pが演算される。

【0010】

【発明が解決しようとする課題】

図31～図37に示した各モードの暗号化装置及び復号装置は、前のブロックデータの暗号化復号されたデータをフィードバックさせて次のブロックデータの暗号化復号処理に利用しなければならないため、一旦暗号化処理又は復号処理が

スタートしてしまうと、その全体の処理が終了しない限り、他の暗号化処理又は復号処理をスタートさせることができないという課題があった。従って、先にスタートした暗号化復号処理が長時間要するものである場合には、後からスタートする暗号化復号処理が長時間待たされてしまうという課題があった。

【0011】

また、暗号化復号されるデータが準備される時間に比べて、暗号化復号処理に要する時間が短い場合には、暗号化復号化装置にアイドル時間が発生してしまうという課題があった。

【0012】

また、秘匿処理と完全性保証処理を行う場合には、秘匿処理を行ってから完全性保証処理を行わなければならず、処理時間がかかるてしまうという課題があった。

【0013】

この発明の好適な実施の形態によれば、あるデータの暗号化復号処理の最中に他のデータの暗号化復号処理を行える暗号化装置、復号装置及び暗号化方法及び復号方法を得ることを目的とする。

【0014】

また、この発明の好適な実施の形態においては、優先度の高いデータの暗号化復号を優先的に行えるようにすることを目的とする。

【0015】

また、この発明の好適な実施の形態においては、秘匿処理と完全性保証処理を並列的に高速に行えるようにすることを目的とする。

【0016】

【課題を解決するための手段】

この発明に係る暗号化装置は、1つ以上のブロックデータからなる第1の処理データと、1つ以上のブロックデータからなる第2の処理データとの暗号化処理をする暗号化装置において、

暗号化処理の状態を記憶するメモリを備え、

第1の処理データの全ブロックデータの暗号化処理が完了する前に第2の処理

データの最初のブロックデータの暗号化処理を開始するとともに、第2の処理データの最初のブロックデータの暗号化処理を開始する場合に第1の処理データの暗号化処理の状態を上記メモリに記憶させ、第1の処理データの暗号化処理を再開する場合に暗号化装置の暗号化処理の状態をメモリに記憶した第1の処理データの暗号化処理の状態に復帰させてから第1の処理データの暗号化処理を再開することを特徴とする。

【0017】

上記暗号化装置は、第2の処理データの全ブロックデータの暗号処理の完了する前に第1の処理データの暗号化処理を再開するとともに、上記メモリは、第1の処理データの暗号化処理を再開する場合に第2の処理データの暗号化処理状態を記憶し、第2の処理データの暗号化処理を再開する場合は、暗号化装置の暗号化処理の状態をメモリに記憶した第2の処理データの暗号化処理の状態に復帰させてから第2の処理データの暗号化処理を再開することを特徴とする。

【0018】

上記第1の処理データは、第1の平文であり、上記第2の処理データは、第2の平文であることを特徴とする。

【0019】

上記暗号化装置は、割り込みにより第2の処理データの最初のブロックデータの暗号化処理を開始することを特徴とする。

【0020】

この発明に係る暗号化装置は、平文Mを構成する平文ブロックデータ M_i ($i = 1, 2, 3, \dots$) と平文Nを構成する平文ブロックデータ N_j ($j = 1, 2, 3, \dots$) とを暗号化する暗号化装置において、

平文Mの暗号化処理中に平文Nの暗号化要求を平文Mの暗号化処理完了前に受け付けるメカニズムと、

暗号化処理を行い中間ブロックデータ T_i 又は暗号文ブロックデータ C_i を出力する暗号化モジュールと、

暗号化モジュールから出力された中間ブロックデータ T_i 又は暗号文ブロックデータ C_i をフィードバックラインを介し暗号化モジュールにフィードバックす

るフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記平文Nの暗号化要求を受け付け、平文Nのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されない場合、フィードバックされるブロックデータを記憶するメモリと、

平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化される場合は、上記フィードバックループのフィードバックラインによりフィードバックされるブロックデータを選択してフィードバックループに供給し、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されず、平文Nのいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリに記憶されたブロックデータを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする。

【0021】

上記メモリは、

複数の平文に対応した複数のレジスタと、

暗号化処理をする平文に対してレジスタを切り替えるスイッチとを備えたことを特徴とする。

【0022】

この発明に係る暗号化方法は、暗号化モジュールを用いて第1の平文Mの平文ブロックデータ M_i ($i = 1, 2, 3, \dots$)を暗号化する工程と、

上記平文ブロックデータ M_i を暗号化している途中で又は平文ブロックデータ M_i を暗号化した後に、第1の平文Mの平文ブロックデータ M_{i+1} の暗号化に用いられる中間ブロックデータ T_i 又は暗号文ブロックデータ C_i をメモリに記憶する工程と、

上記平文ブロックデータ M_{i+1} の暗号化に用いられるブロックデータをメモリに記憶した後に、第2の平文Nの少なくとも1つの平文ブロックデータを暗号化する工程と、

上記第2の平文Nの少なくとも1つの平文ブロックデータを暗号化した後に、メモリに記憶された、平文ブロックデータ M_{i+1} の暗号化に用いられるブロックデータを入力し、暗号化モジュールを用いて第1の平文Mの平文ブロックデータ M_{i+1} を暗号化する工程と
を備えたことを特徴とする。

【0023】

この発明に係る暗号化装置は、1つ以上の平文ブロックデータからなる平文を暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、

平文ブロックデータを暗号化したときに生成した中間ブロックデータ T_i 又は暗号文ブロックデータ C_i をフィードバックする第1のフィードバックループを有し、平文ブロックデータを入力し、第1のフィードバックループによりブロックデータをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化部と、

認証子演算途中結果をフィードバックする第2のフィードバックループを有し、暗号化部から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第2のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成部と
を備えたことを特徴とする。

【0024】

上記暗号化部と認証子生成部とは、1つの暗号化モジュールと、1つのフィードバックループとを兼用して暗号化処理と認証子生成処理とを交互に行うとともに、

上記1つのフィードバックループは、
暗号化処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、
暗号化処理と認証生成処理とを交互に実行するために、メモリから暗号化処理と認証子生成処理との結果を交互に選択して暗号化モジュールに出力するセレクタと

を備えたことを特徴とする。

【0025】

この発明に係る暗号化方法は、1つ以上の平文ブロックデータからなる平文を暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化方法において、

平文ブロックデータを暗号化したときに生成した中間ブロックデータ T_i 又は暗号文ブロックデータ C_i をフィードバックする第1のフィードバック工程を有し、平文ブロックデータを入力し、第1のフィードバックループによりブロックデータをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化工程と、

認証子演算途中結果をフィードバックする第2のフィードバック工程を有し、暗号化工程から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第2のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成工程と

を備えたことを特徴とする。

【0026】

この発明に係る復号装置は、1つ以上のブロックデータからなる第1の処理データと、1つ以上のブロックデータからなる第2の処理データとの復号処理をする復号装置において、

復号処理の状態を記憶するメモリを備え、

第1の処理データの全ブロックデータの復号処理が完了する前に第2の処理データの最初のブロックデータの復号処理を開始するとともに、第2の処理データの最初のブロックデータの復号処理を開始する場合に第1の処理データの復号処理の状態を上記メモリに記憶させ、第1の処理データの復号処理を再開する場合に復号装置の復号処理の状態をメモリに記憶した第1の処理データの復号処理の状態に復帰させてから第1の処理データの復号処理を再開することを特徴とする。

【0027】

上記復号装置は、第2の処理データの全ブロックデータの復号処理の完了する前に第1の処理データの復号処理を再開するとともに、上記メモリは、第1の処理データの復号処理を再開する場合に第2の処理データの復号処理状態を記憶し、第2の処理データの復号処理を再開する場合は、復号装置の復号処理の状態をメモリに記憶した第2の処理データの復号処理の状態に復帰させてから第2の処理データの復号処理を再開することを特徴とする。

【0028】

上記第1の処理データは、第1の暗号文であり、上記第2の処理データは、第2の暗号文であることを特徴とする。

【0029】

上記復号装置は、割り込みにより第2の処理データの最初のブロックデータの復号処理を開始することを特徴とする。

【0030】

この発明に係る復号装置は、暗号文Cを構成する暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$)と暗号文Nを構成する暗号文ブロックデータ N_j ($j = 1, 2, 3, \dots$)とを復号する復号装置において、

暗号文Cの復号処理中に暗号文Nの復号要求を任意の時点で受け付けるメカニズムと、

復号処理を行い中間ブロックデータ T_i 又は平文ブロックデータ M_i を出力する復号モジュールと、

復号モジュールから出力された中間ブロックデータ T_i 又は平文ブロックデータ M_i をフィードバックラインを介し復号モジュールにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記暗号文Nの復号要求を受け付け、暗号文Nのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されない場合、フィードバックされるブロックデータを記憶するメモリと、

暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号さ

れる場合は、上記フィードバックループのフィードバックラインによりフィードバックされるブロックデータを選択してフィードバックループに供給し、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されず、暗号文Nのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリに記憶されたブロックデータを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする。

【0031】

上記メモリは、
複数の暗号文に対応した複数のレジスタと、
復号処理をする暗号文に対応してレジスタを切り替えるスイッチと
を備えたことを特徴とする。

【0032】

この発明に係る復号方法は、復号モジュールを用いて第1の暗号文Cの暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$)を復号する工程と、
上記暗号文ブロックデータ C_i を復号している途中で又は暗号文ブロックデータ C_i を復号した後に、第1の暗号文Cの暗号文ブロックデータ C_{i+1} の復号に用いられる中間ブロックデータ T_i 又は平文ブロックデータ M_i をメモリに記憶する工程と、

上記暗号文ブロックデータ C_{i+1} の復号に用いられるブロックデータをメモリに記憶した後に、第2の暗号文Nの少なくとも1つの暗号文ブロックデータを復号する工程と、

上記第2の暗号文Nの少なくとも1つの暗号文ブロックデータを復号した後に、メモリに記憶された、暗号文ブロックデータ C_{i+1} の復号に用いられるブロックデータを入力し、復号モジュールを用いて第1の暗号文Cの暗号文ブロックデータ C_{i+1} を復号する工程と
を備えたことを特徴とする。

【0033】

この発明に係る復号装置は、1つ以上の暗号文ブロックデータからなる暗号文

を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、

暗号文ブロックデータを復号したときに生成した中間ブロックデータ T_i 又は平文ブロックデータ M_i をフィードバックする第1のフィードバックループを有し、暗号文ブロックデータを入力し、第1のフィードバックループによりブロックデータをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号部と、

認証子演算途中結果をフィードバックする第2のフィードバックループを有し、復号部に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第2のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成部と
を備えたことを特徴とする。

【0034】

上記復号部と認証子生成部とは、1つの復号モジュールと、1つのフィードバックループとを兼用して復号処理と認証子生成処理とを交互に行うとともに、

上記1つのフィードバックループは、

復号処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

復号処理と認証生成処理とを交互に実行するために、メモリから復号処理と認証子生成処理との結果を交互に選択して復号モジュールに出力するセレクタと
を備えたことを特徴とする。

【0035】

この発明に係る復号方法は、1つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号方法において、

暗号文ブロックデータを復号したときに生成した中間ブロックデータ T_i 又は平文ブロックデータ M_i をフィードバックする第1のフィードバック工程を有し、暗号文ブロックデータを入力し、第1のフィードバックループによりブロックデータをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復

号工程と、

認証子演算途中結果をフィードバックする第2のフィードバック工程を有し、復号工程に入力される暗号文のブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第2のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成工程とを備えたことを特徴とする。

【0036】

【発明の実施の形態】

実施の形態1.

図1は、この実施の形態におけるCBCモードの暗号化装置を示す図である。この実施の形態の暗号化装置は、セレクタ54と排他的論理和回路58と暗号鍵Kを用いた暗号化モジュール51とメモリ55とにより構成されている。セレクタ54と排他的論理和回路58と暗号鍵Kを用いた暗号化モジュール51は、フィードバックライン65とフィードバックライン66とフィードバックライン67によりフィードバックループを構成している。暗号鍵Kを用いた暗号化モジュール51により暗号化された暗号文ブロックデータC_iは、フィードバックループにより再び排他的論理和回路58に入力され、暗号鍵Kを用いた暗号化モジュール51に供給される。

【0037】

メモリ55は、フィードバックライン65と並列に設けられている。メモリ55は、レジスタ56とスイッチ57により構成されている。スイッチ57は、暗号鍵Kを用いた暗号化モジュール51の出力をレジスタ56に入力させるか無視するかを切り替えるものである。この切り替えは、例えば、割り込みITにより行われる。割り込みITが発生した場合には、スイッチ57はEに接続され、割り込みITが解除された場合には、スイッチ57はFに接続される。レジスタ56は、Eを経由してきた暗号文ブロックデータC_iを入力して記憶するものである。レジスタ56に記憶された暗号文ブロックデータC_iは、セレクタ54に出力される。セレクタ54は、A、B、Cの3つの入力を有しており、いずれか1

つの入力を選択するものである。これらの選択は、後述するように割り込みITに依存する。

【0038】

図2は、図1に示した暗号化装置の動作手順を示す図である。

図3は、図1に示した暗号化装置の動作フローチャートである。

この暗号化装置が電源を投入された場合のセレクタ54の入力はAに設定されており、スイッチ57はEに接続されているものとする。また、平文Nの暗号化要求があるときは、割り込みITが発生し、平文Nの暗号化要求が解除されるまで、割り込みITがオンになり続けるものとする。時刻T0において、平文ブロックデータM₁の暗号化処理がスタートする。時刻T0において、平文ブロックデータM₁の暗号化がスタートした場合には、セレクタ54の入力Aから一旦インシャルバリューIVが入力された後、セレクタ54はBに切り替わる。そして、時刻Xにおいて、平文ブロックデータN₁の暗号化を要求する割り込みITが発生したとする。時刻T1までに、暗号文ブロックデータC₁はメモリ55に記憶された状態になる。そして、割り込みITの発生により時刻T1において、セレクタ54は入力をAに設定する。また、時刻T1において、スイッチ57はFに接続される。時刻T1以降は、平文ブロックデータN₁の暗号化が行われ、暗号文ブロックデータD₁が出力される。時刻Yにおいて、平文ブロックデータN₁の暗号化が終了し、割り込みITが解除されたものとする。この割り込みITの解除により時刻T2において、セレクタ54の入力はCに切り替えられ、スイッチ57はEに接続される。セレクタ54がCに切り替わったことにより、メモリ55に記憶されていた暗号文ブロックデータC₁が平文ブロックデータM₂の暗号化のために入力され、鍵Kを用いた暗号化モジュール51により平文ブロックデータM₂が暗号化されて、暗号文ブロックデータC₂が出力される。時刻T3以前においては、セレクタ54の入力はBに切り替えられ、平文ブロックデータM₃を暗号化する場合には、フィードバックループのフィードバックライン65からフィードバックされた暗号文ブロックデータC₂が入力され、鍵Kを用いた暗号化モジュール51により平文ブロックデータM₂が暗号化されて、平文ブロックデータM₃が暗号化され、暗号文ブロックデータC₃が出力される。

【0039】

図3のフローチャートを用いて全体の動作を説明する。

S1において、平文Mの暗号化処理がスタートし続行される。最後のブロックデータまで処理を終えた場合には、処理を終了する。S2において、任意の時点で生じる割り込みITの発生が監視される。割り込みITの発生がない場合には、S1の処理が続行される。平文ブロックデータM_iの処理中に割り込みITが発生した場合には、S3において、現在処理中の平文ブロックデータM_iの暗号文ブロックデータC_iをメモリ55のレジスタ56に記憶する。S4において、割り込みITにより暗号化処理の要求があった平文Nの暗号化処理を行う。このS4の暗号化処理は、S5に示すように、割り込みITの解除があるまで連続して行われる。割り込みITの解除があった場合には、S6において、メモリ55のレジスタ56に記憶した暗号文ブロックデータC_iを用いてM_{i+1}の暗号化処理を行う。それ以降の処理は、S1に戻り、暗号化処理が続行される。

【0040】

図4は、セレクタ54のオペレーション処理を示す図である。

電源がオンになった場合には、S11に示すように、入力をAに設定する。S12において、暗号化がスタートした場合には、S13において、入力をBに設定する。即ち、フィードバックループのフィードバックライン65によりフィードバックされる暗号文ブロックデータC_iが用いられる。S14において、現在処理しているブロックデータが最後であるということが判定された場合には、S11に戻り電源オンと同じ状態に戻る。S15において、割り込みITの発生が確認された場合には、S16において、入力をAに設定し、暗号化がスタートした場合には、S18において、入力をBに設定する。割り込みITの解除があるまでは、入力がBに設定されたままで動作する。即ち、フィードバックループのフィードバックライン65によりフィードバックされる暗号文ブロックデータC_iが用いられる。S19において、割り込みITの解除があったことが検知された場合には、S20において、入力をCに設定する。この入力をCに設定することにより、メモリ55に記憶された暗号文ブロックデータC_iが入力されることになる。このCからの入力による暗号化がスタートした場合には、S13に戻り

入力をBに設定する。

このようにして、割り込みITの発生に基づき、セレクタ54を切り替えることができる。

なお、平文Mの暗号化処理も、割り込みITにより任意の時刻にスタートさせてもよい。

【0041】

図5は、スイッチ57の割り込み処理のフローチャートである。

電源がオンになった場合、そして、その後の最初の平文の暗号化処理の場合は、スイッチ57はEに接続される。そして、S31において、割り込みITが発生した場合には、スイッチ57をEからFに接続する。そして、S33において、割り込みITの解除が検出された場合には、スイッチ57をFからEに接続する。このようにして、スイッチ57は、割り込みITの発生から解除までは暗号文ブロックデータC_iを無視する。従って、メモリ55のレジスタ56には、割り込みITが発生したときに生成された暗号文ブロックデータC_iが記憶され続けることになる。

【0042】

メモリ55は、割り込みITが発生したときの暗号化装置の状態を記憶するメモリである。メモリ55が暗号化処理の状態を記憶しておくことにより、あるデータの暗号化の最中に他のデータの暗号化を行った場合でも、再びあるデータの暗号化の処理に復帰することができる。即ち、メモリ55に記憶されたデータを用いることにより、暗号化が中断されたときと全く同じ状態に暗号化装置を復帰させることができ、中断した暗号化処理を続行させることができる。

【0043】

図6は、メモリ55の他の例を示す図である。

メモリ55は、割り込み制御部52と入力スイッチ96と出力スイッチ97と複数のレジスタ（REG1, 2, 3）を有している。このように、複数のレジスタを有することにより、複数の割り込みを受け付けることが可能になる。

【0044】

図7は、メモリ55の割り込み処理の動作を示す図である。

割り込み I T が発生すると、S 4 1において、現在使用中のレジスタ k の番号 k を記憶する。S 4 2において、入力スイッチ 9 6 と出力スイッチ 9 7 をレジスタ k 以外のレジスタ 1 に接続する。この状態で、平文 N の暗号化が継続される。更に、平文 N の暗号化の最中に他の割り込みが発生したかを監視する。S 4 3において、他の割り込み I T が発生したことが検出された場合には、再び自分自身である S 4 0 の処理を呼び出す。このように、割り込み I T が発生するたびに、自分自身を S 4 0 の処理をリカーシブに呼び出すことにより、複数階層の割り込み処理を行うことができる。S 4 4においては、割り込みが解除されたかを検出し、割り込みが解除された場合には、入力スイッチ 9 6 と出力スイッチ 9 7 を記憶しておいた番号 k を用いてレジスタ k に切り替える。図 6 に示す場合は、3 つのレジスタがあるので、3 階層の割り込み処理を行うことができる。

【0045】

図 8 は、メモリ 5 5 の他の例を示す図である。

メモリ 5 5 は、スタック 6 4 を有している。スタック 6 4 は、先入れ後出し (FIFO) のレジスタである。スタック 1 を使用中に割り込み I T が発生した場合には、スタック 1 のデータをスタック 2 に移し、それ以後のデータをスタック 1 に積み上げ、割り込み I T が解除された場合には、積み上げたスタック 1 のデータを出力し、スタック 2 のデータをスタック 1 に戻す。図 8 に示す場合は、4 階層の割り込み処理を行える場合を示している。

【0046】

図 6 に示すように、複数階層の割り込み処理を行うことができる場合は、各割り込みに対して優先度を付けることができる。例えば、割り込み I T 1 を優先度 1 とし、割り込み I T 2 を優先度 I より優先度の低い優先度 2 とすることにより、優先度 1 の割り込み I T 1 が発生した場合には、優先度 2 の処理を遅らせることができる。

【0047】

図 9 は、優先度 1 の暗号化処理を優先度 2 の暗号化処理に優先させた場合を示している。優先度 1 の暗号化処理を先に終了させている。

図 10 は、優先度がともに等しい場合の暗号化処理の場合を示している。

優先度が等しい場合には、2つの平文の各ブロックデータを交互に暗号化する。

図11は、優先度1のデータと2つの優先度2のデータを暗号化する場合を示している。

図9～図11に示すように、割り込みに優先度を付けることによりユーザが望ましいと思われる暗号化処理手順を実現することができる。緊急用のデータや短いデータの場合には、優先度を高くすることにより効率のよい処理を行うことができる。

【0048】

図12は、メモリ55をフィードバックライン66と並列においていた場合を示している。

第1セレクタ61と第2セレクタ62とにより、図1のセレクタ54と同じ選択動作をさせる。

図13は、メモリ55をフィードバックライン67と並列においていた場合を示している。

図14は、図13の暗号化装置の動作手順を示す図である。

割り込みITが発生した時刻Xが排他的論理回路58で排他的論理演算される前である場合には、メモリ55は、排他的論理回路58により排他的論理演算された中間ブロックデータ T_i を記憶する。そして、平文ブロックデータ N_1 を暗号化する。次に、メモリ55に記憶された中間ブロックデータ T_i を第2セレクタ62により選択させ、暗号鍵Kを用いた暗号化モジュール51に入力し、暗号化して暗号文ブロックデータ C_1 を出力する。

【0049】

図1及び図12及び図13に示すように、メモリ55は、フィードバックライン65とフィードバックライン66とフィードバックライン67のいずれのラインと並列の設けられていても構わない。メモリ55は、暗号化装置が、あるデータの暗号化処理中に他のデータの暗号化を開始するとき、他のデータの暗号化を開始する直前の状態を覚えておくものであり、他のデータの暗号化処理が終了した時点で、メモリ55に記憶されたデータを用いて暗号化装置が元の状態に復帰

できるのであれば、メモリ55は、どの場所に設けられていても構わない。また、メモリ55は、複数箇所に設けられていてもよい。

【0050】

図15は、OFBモードの暗号化装置の構成図である。

図34に比べて、メモリ55が追加されている点が特徴である。

図16は、CFBモードの暗号化装置を示す図である。

図36に比べて、メモリ55が設けられている点が特徴である。

【0051】

図17は、CBCモードの復号装置を示す図である。

図33に比べて、メモリ75が設けられている点が特徴である。

メモリ75は、レジスタ76とスイッチ77により構成されている。

図18は、図17の復号装置の動作手順を示す図である。

暗号文ブロックデータ C_1 を復号している最中に割り込みITの発生があった場合には、暗号文ブロックデータ C_1 がメモリ75のレジスタ76に記憶される。その後、暗号文ブロックデータ D_1 の復号が行われ、平文ブロックデータ N_1 が復号される。そして、メモリ75のレジスタ76に記憶された暗号文ブロックデータ C_1 が読み出され、暗号文ブロックデータ C_2 の復号が行われ、平文ブロックデータ M_2 が復号される。セレクタ74の動作は、図4に示したものと同じである。また、スイッチ77の動作は、図5に示したものと同じである。

【0052】

図19は、OFBモードの復号装置を示す図である。

図20は、CFBモードの復号装置を示す図である。

【0053】

前述した説明においては、3つのモードの場合の暗号化装置と復号装置を説明したが、前述した3つのモードは一例であり、これらのモードの改良されたもの、或いは、これらのモードが変形されたものであっても構わない。特に、特徴となる点は、先のブロックデータが暗号化復号されたときに生成されたブロックデータ C_i 又は M_i 又は T_i が次のブロックデータ M_{i+1} 又は C_{i+1} の暗号化復号処理にフィードバックデータとして用いられる暗号化復号方法において、暗号化

復号の状態を記憶するメモリ55を設け、他のデータの暗号化復号化の処理後にブロックデータC_i又はM_i又はT_iを用いて再び元の状態に復帰可能にできる点である。従って、特に暗号化モード、復号モードは問わない。

なお、割り込みI Tを用いず、ポーリング方式やトークン取得方式等の他のメカニズムを用いて暗号化要求を受け付け、2以上の暗号化復号処理のインタラクティブな並列処理を行うようにしてもよい。

また、暗号鍵Kを用いる暗号化復号処理の場合を示したが、暗号鍵Kを用いない暗号化復号処理の場合でもよい。

【0054】

実施の形態2.

この実施の形態においては、暗号化装置が秘匿処理とデータの完全性保証処理を行う場合について説明する。

データの秘匿処理とは、データを暗号化し、データが盗聴されても、或いは、盗まれても意味が分からなくなることである。また、データの完全性保証とは、データが何者かにより置き換えられていることがないことを保証することをいう。データを伝送する場合には、データの秘匿処理を行った上にデータの完全性を保証して伝送したい場合がある。データの秘匿処理は、データを暗号化することにより行われる。データの完全性保証処理は、データの最後に認証子(MAC: Message Authentication Code)を付加し、その認証子を検証することにより改竄を発見することにより行われる。

【0055】

図21は、OFBモードの暗号化部100により秘匿処理を行い、CBCモードの認証子生成部200により認証子(MAC)を生成する場合を示している。

図22は、図21に示す暗号化装置の動作手順を示す図である。

平文ブロックデータM₁が、まず暗号文ブロックデータC₁に暗号化される。次に、平文ブロックデータM₂が入力され、暗号文ブロックデータC₂に暗号化される。この平文ブロックデータM₂の暗号化と同じ時刻に暗号文ブロックデータC₁が入力され、認証子の演算が始まる。時刻T1とT2の間に平文ブロックデータM₂の暗号化と暗号文ブロックデータC₁に基づく認証子演算が行われる

。また、時刻T2とT3の間では、平文ブロックデータ M_3 の暗号化と暗号文ブロックデータ C_2 に基づく認証子の演算が行われる。時刻T3においては、暗号文ブロックデータ C_3 に基づく認証子の演算が行われ、認証子Pが出力される。

図21で特徴となる点は、排他的論理和回路58から出力される暗号文ブロックデータ C_i がフィードライン69により排他的論理和回路59に入力されている点である。フィードライン69によりOFBモードとCBCモードの暗号化処理を結合することにより、図22に示すように、秘匿処理と完全性認証処理がパイプライン処理で実行される。図41に示した場合は、時刻T6で処理時間がかかったが、図22の場合は、時刻T4で処理が終了して高速処理が行われたことになる。

【0056】

図23は、図21に示した暗号化装置の動作フローチャート図である。

S51において、ブロックデータカウンタ i を1とする。S52は、暗号化部100の動作であり、暗号化部100は、平文ブロックデータ M_i を入力して平文ブロックデータ M_i を暗号化し、暗号文ブロックデータ C_i を生成して暗号文ブロックデータ C_i を出力する。S53は、認証子生成部200の動作であり、暗号文ブロックデータ C_i を入力し暗号文ブロックデータ C_i を暗号化し、認証子を演算する。S54は、ブロックデータカウンタ i が最後のブロックデータ n を示しているかどうかを判断し、最後のブロックデータでない場合には、S55において、ブロックデータカウンタ i を増加させ、再びS52の処理に戻る。即ち、暗号化部100と認証子生成部200の処理を繰り返す。S54において、最後のブロックデータの処理が終了した場合には、S53で演算された直前の認証子が最終的な認証子であるから、S56において、その認証子を暗号文ブロックデータ C_i の最後に付加する。図23に示すように、暗号化部100が暗号文ブロックデータ C_i を生成するたびに、認証子生成部200が暗号文ブロックデータ C_i を入力して認証子を演算することによりパイプライン処理が可能になり、高速処理が行われる。

【0057】

図24は、図21に示した暗号化部100と認証子生成部200をあわせたも

のである。即ち、暗号化部100と認証子生成部200の暗号化モジュール51を兼用し、また、暗号化部100と認証子生成部200の排他的論理回路58と59を兼用したものである。更には、暗号化部100のフィードバックライン65と認証子生成部200のフィードバックライン66を兼用したものである。

【0058】

第1セレクタ61は、秘匿処理の開始時にイニシャルバリューIVを選択するものである。第2セレクタ62は、完全性保証処理の開始時にイニシャルバリューIVを選択するものである。第3セレクタ63は、秘匿処理と完全性保証処理を交互に選択するものである。第3セレクタ63は入力をEにすることにより、秘匿処理を行わせることができる。また、第3セレクタ63は入力をFにすることにより、完全性保証処理を行わせることができる。

メモリ93は、暗号鍵Kを用いた暗号化モジュール51から出力された中間ブロックデータ T_i を記録するものである。メモリ93は、入力スイッチ96と出力スイッチ97と第1レジスタ98と第2レジスタ99により構成されている。入力スイッチ96と出力スイッチ97は、第3セレクタ63の切り替えと同期しており、第3セレクタ63が切り替わるたびに入力スイッチ96及び出力スイッチ97も切り替わる。

【0059】

図25は、図24に示す暗号化装置の動作手順を示す図である。

時刻T0とT1の間で平文ブロックデータ M_1 の秘匿処理が行われる。秘匿処理の途中で生成された中間ブロックデータは、第1レジスタ98に記憶される。時刻T1とT2の間では、暗号文ブロックデータ C_1 に基づく認証子の演算が行われる。完全性保証処理により生成された認証子演算途中結果は、第2レジスタ99に記憶される。次に、時刻T2とT3の間では、第1レジスタ98に記憶された中間ブロックデータと平文ブロックデータ M_2 に基づいて平文ブロックデータ M_2 の秘匿処理が行われる。次に、時刻T3とT4の間では、第2レジスタ99に記憶された認証子中間演算結果と暗号文ブロックデータ C_2 が入力され、認証子の演算が行われる。この動作を繰り返すことにより、秘匿処理と完全性認証処理が完了し、暗号文と認証子Pが出力される。図25に示す場合は、時刻T6

まで処理が終了し、時間の短縮は図られていないが、図24に示すように、暗号鍵Kを用いた暗号化モジュール51と排他的論理和回路58とフィードバックライン67, 68(フィードバックループ)が兼用されているので、回路規模を小さくすることができる。

【0060】

図26は、OFBモードの復号化部300とCBCモードの認証子生成部400を有する復号装置を示す図である。

この認証子生成部400は、認証子生成部200と同一構成のものである。

暗号文ブロックデータ C_i は、復号化部300の排他的論理和回路78に入力されると同時に、フィードライン69により認証子生成部400に入力される。このような構成により、復号化部300と認証子生成部400の処理が同時並列実行され、処理速度が向上する。

【0061】

図27は、図26に示した復号装置の復号化部300と認証子生成部400を一体化したものである。

図27は、暗号鍵Kを用いた復号モジュール71とフィードバックライン87, 88(フィードバックループ)が兼用されている場合を示している。

第1セレクタ81は、復号処理の開始時にイニシャルバリューIVを選択するものである。第2セレクタ82は、完全性保証処理の開始時にイニシャルバリューIVを選択するものである。第3セレクタ83は、復号処理と完全性保証処理を交互に選択するものである。第3セレクタ83は入力をEにすることにより、復号処理を行わせることができる。また、第3セレクタ83は入力をFにすることにより、完全性保証処理を行わせることができる。

メモリ93は、暗号鍵Kを用いた暗号化モジュール51から出力された中間ブロックデータ T_i を記録するものである。メモリ93は、入力スイッチ96と出力スイッチ97と第1レジスタ98と第2レジスタ99により構成されている。入力スイッチ96と出力スイッチ97は、第3セレクタ83の切り替えと同期しており、第3セレクタ83が切り替わるたびに入力スイッチ96及び出力スイッチ97も切り替わる。

【0062】

図28は、図27に示した復号装置の動作手順を示す図である。

時刻T0とT1の間で暗号文ブロックデータC₁の復号処理と暗号文ブロックデータC₁のレジスタ111への保存が行われる。復号処理の途中で生成された中間ブロックデータは、第1レジスタ98に記憶される。時刻T1とT2の間では、レジスタ111に保存された暗号文ブロックデータC₁に基づく認証子の演算が行われる。完全性保証処理により生成された認証子演算途中結果は、第2レジスタ99に記憶される。次に、時刻T2とT3の間では、暗号文ブロックデータC₂がレジスタ111に保存され、第1レジスタ98に記憶された中間ブロックデータと暗号文ブロックデータC₂に基づいて平文ブロックデータM₂の復号処理が行われる。次に、時刻T3とT4の間では、第2レジスタ99に記憶された認証子中間演算結果とレジスタ111に保存された暗号文ブロックデータC₂が入力され、認証子の演算が行われる。この動作を繰り返すことにより、復号処理と完全性認証処理が完了し、平文と認証子Pが出力される。

【0063】

図29は、前述した暗号化装置又は復号装置の実装形式を示す図である。

図29は、FPGA又はIC又はLSIの中に前述した暗号化装置及び復号装置が実現されている場合を示している。即ち、前述した暗号化装置及び復号装置は、ハードウェアで実現することができる。また、図示していないが、プリントサーキットボードにより実現することも可能である。

【0064】

図30は、前述した暗号化装置及び復号装置をソフトウェアで実現する場合を示している。

前述した暗号化装置は、暗号化プログラム47で実現することができる。暗号化プログラム47は、ROM42に記憶されている。暗号化プログラム47は、サブルーチンとして機能する。暗号化プログラム47は、RAM45に記憶されたアプリケーションプログラム46からサブルーチンコールにより呼び出されて実行される。或いは、暗号化プログラム47は、割り込み制御部43で受け付ける割り込みの発生により起動されるようにしても構わない。メモリ55は、RA

M4.5の一部であっても構わない。アプリケーションプログラム4.6、暗号化プログラム4.7は、CPU4.1により実行されるプログラムである。

【0065】

図3.1は、アプリケーションプログラム4.6が暗号化プログラム4.7を呼び出すメカニズムを示している。

アプリケーションプログラム4.6は、鍵KとイニシャルバリューIVと平文Mと暗号文Cをパラメータにして暗号化プログラム4.7を呼び出す。暗号化プログラム4.7は、鍵KとイニシャルバリューIVと平文Mを入力し、暗号文Cを返すものである。暗号化プログラム4.7と復号プログラムが同一のときは、鍵KとイニシャルバリューIVと暗号文Cと平文Mをパラメータにして暗号化プログラム4.7を呼び出す。

また、図示しないが、暗号化プログラム4.7は、デジタルシグナルプロセッサと、そのデジタルシグナルプロセッサにより読み込まれて実行されるプログラムによって実現しても構わない。即ち、ハードウェアとソフトウェアの組み合わせによって暗号化プログラム4.7を実現しても構わない。

【0066】

図2.9、図3.0、図3.1は、主として、暗号化装置の場合を説明したが、復号装置でも同様の方式で実現できる。

【0067】

図2.9及び図3.0に示したような暗号化装置及び復号装置は、電子機器に対してインストールすることができる。例えば、パーソナルコンピュータやファクシミリ装置や携帯電話やビデオカメラやデジタルカメラやテレビカメラ等のあらゆる電子機器にインストールすることができる。特に、この実施の形態における特徴が発揮できるのは、複数のチャネルからのデータを暗号化復号する場合に有効である。或いは、複数のユーザからのデータがアットランダムに到着して復号する場合に、或いは、複数のユーザに対するデータがアットランダムに発生して、それぞれのデータをリアルタイムに暗号化するような場合に有効である。即ち、暗号化復号するデータの数に比べて暗号化復号する装置の数が少ない場合に、前述した実施の形態の暗号化装置、復号装置が非常に有効である。例えば、多くの

クライアントコンピュータをサポートしなければならないサーバコンピュータや多くの携帯電話機からのデータを集配しなければならない基地局や回線コントローラなどに、前述した暗号化装置や復号装置が非常に有効である。

【0068】

なお、暗号化処理同士及び復号処理同士の並列処理でなく、暗号化処理と復号処理との並列処理を行うようにしてもよい。

【0069】

また、OFBモードの暗号化部（又は復号化部）とCBCモードの認証子生成部との組み合わせの場合を示したが、OFBモードとCBCモードとCFBモードとこれらのモードの改良モードとその他のモードとのいずれのモードの組み合わせでも構わない。

【0070】

また、認証子生成部が、暗号鍵Kを用いた暗号化を行う場合を示したが、認証子生成部は、データの攪拌や演算やその他のデータ処理を行う場合であっても構わない。

【0071】

【発明の効果】

以上のように、この発明の好適な実施の形態によれば、平文Mの暗号化の途中で平文Nの暗号化を開始することができる。また、暗号文Cの復号中に他の暗号文Dの復号を開始することができる。

【0072】

また、この発明の好適な実施の形態によれば、優先度を付けることにより暗号化復号されるデータを優先度に基づいて高速に処理することができる。

【0073】

また、この発明の好適な実施の形態によれば、秘匿処理と完全性保証処理とを並列処理することにより高速処理が行える。また、秘匿処理と完全性保証処理を統合化された1つのハードウェアで行うことができる。

【図面の簡単な説明】

【図1】 実施の形態1のCBCモードの暗号化装置を示す図。

- 【図2】 CBCモードの暗号化装置の動作手順を示す図。
- 【図3】 CBCモードの暗号化装置の動作フローチャート図。
- 【図4】 セレクタ54の動作フローチャート図。
- 【図5】 スイッチ57の割り込み処理フローチャート図。
- 【図6】 メモリ55の他の例を示す図。
- 【図7】 メモリ55の割り込み処理フローチャート図。
- 【図8】 メモリ55の他の例を示す図。
- 【図9】 優先度処理を示す図。
- 【図10】 優先度処理を示す図。
- 【図11】 優先度処理を示す図。
- 【図12】 メモリ55がフィードバックライン66と並列に設けられている図。
- 【図13】 メモリ55がフィードバックライン67に並列に設けられている図。
- 【図14】 図13の暗号化装置の動作手順を示す図。
- 【図15】 OFBモードの暗号化装置を示す図。
- 【図16】 CFBモードの暗号化装置を示す図。
- 【図17】 CBCモードの復号装置を示す図。
- 【図18】 CBCモードの復号装置の動作手順を示す図。
- 【図19】 OFBモードの復号装置を示す図。
- 【図20】 CFBモードの復号装置を示す図。
- 【図21】 実施の形態2の暗号化部100と認証子生成部200を有する暗号化装置を示す図。
- 【図22】 暗号化部100と認証子生成部200を有する暗号化装置の動作手順を示す図。
- 【図23】 暗号化部100と認証子生成部200を有する暗号化装置のフローチャート図。
- 【図24】 暗号化部100と認証子生成部200を1つにした暗号化装置を示す図。

【図25】 暗号化部100と認証子生成部200を1つにした暗号化装置の動作手順を示す図。

【図26】 復号化部300と認証子生成部400を有する復号装置を示す図。

【図27】 復号化部300と認証子生成部400を1つにした復号装置を示す図。

【図28】 復号化部300と認証子生成部400を1つにした復号装置の動作手順を示す図。

【図29】 暗号化装置及び復号装置のハードウェア実現例を示す図。

【図30】 暗号化装置及び復号装置のハードウェア実現例を示す図。

【図31】 アプリケーションプログラム46により暗号化プログラム47が呼び出される場合を示す図。

【図32】 従来のCBCモードの暗号化装置を示す図。

【図33】 従来のCBCモードによる復号装置を示す図。

【図34】 従来のOFBモードの暗号化装置を示す図。

【図35】 従来のOFBモードによる復号装置を示す図。

【図36】 従来のCFBモードの暗号化装置を示す図。

【図37】 従来のCFBモードによる復号装置を示す図。

【図38】 従来の暗号化手順を示す図。

【図39】 従来の暗号化手順を示す図。

【図40】 秘匿処理と完全性保証処理を説明する図。

【図41】 従来の秘匿処理と完全性保証処理の動作手順を示す図。

【符号の説明】

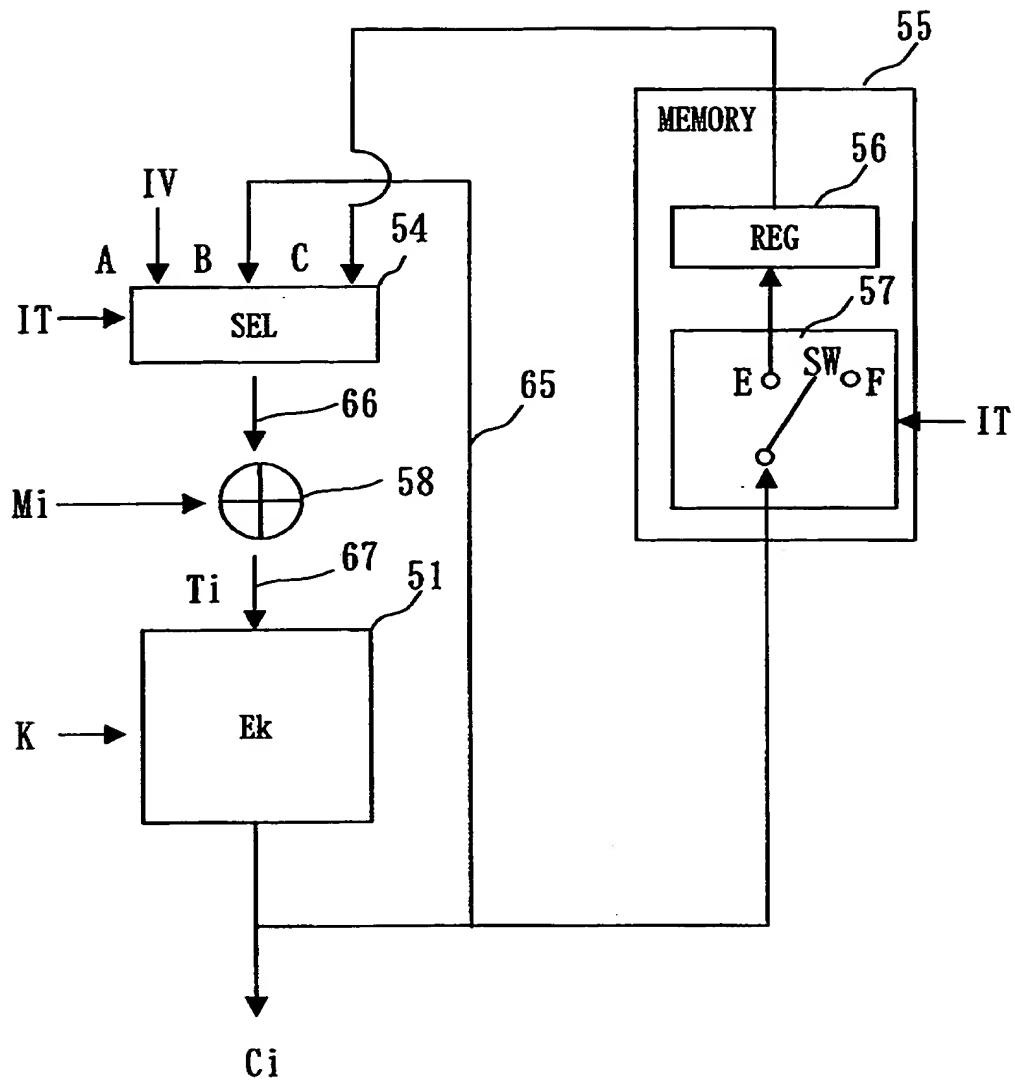
41 CPU、42 ROM、43, 52 割り込み制御部、45 RAM、
 46 アプリケーションプログラム、47 暗号化プログラム、51 暗号鍵K
 を用いた暗号化モジュール、53, 54, 73, 74 セレクタ、55, 75,
 95 メモリ、56, 76 レジスタ、57, 77 スイッチ、58, 59, 7
 8, 79 排他的論理和回路、61, 81 第1セレクタ、62, 82 第2セ
 レクタ、63, 83 第3セレクタ、64 スタック、65, 66, 67, 68

, 85, 86, 87, 88 フィードバックライン、69, 89 フィードライン、71 暗号鍵Kを用いた復号モジュール、93 第1スイッチ、94 第2スイッチ、96 入力スイッチ、97 出力スイッチ、98 第1レジスタ、99 第2レジスタ、111 レジスタ、 C_1, C_2, C_3, C_i, D_1 暗号文ブロックデータ、 F_i フィードバックブロックデータ、IT 割り込み、IV イニシャルバリュー、 N_1, M_1, M_2, M_3, M_i 平文ブロックデータ、P 認証子、T, X, Y 時刻、 T_i 中間ブロックデータ。

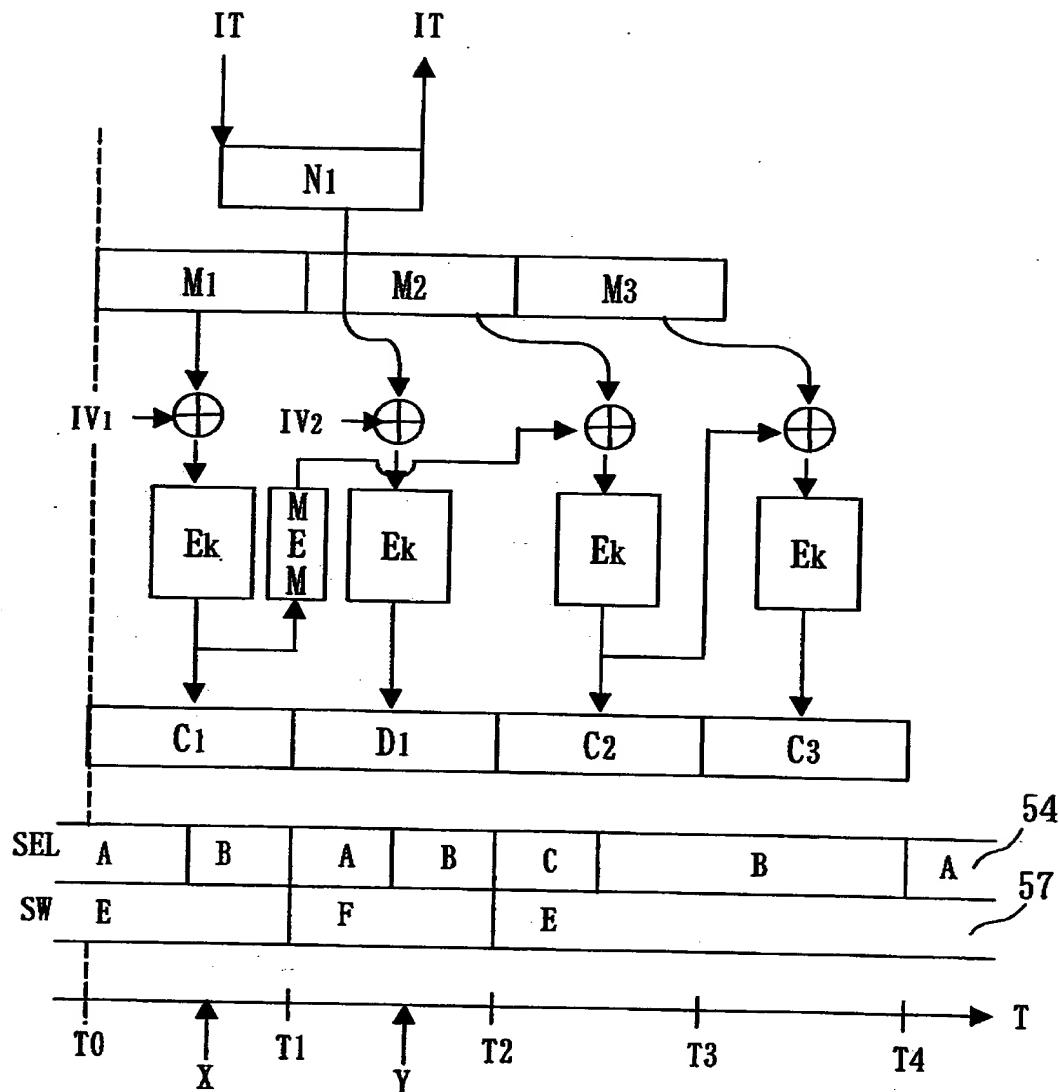
【書類名】

図面

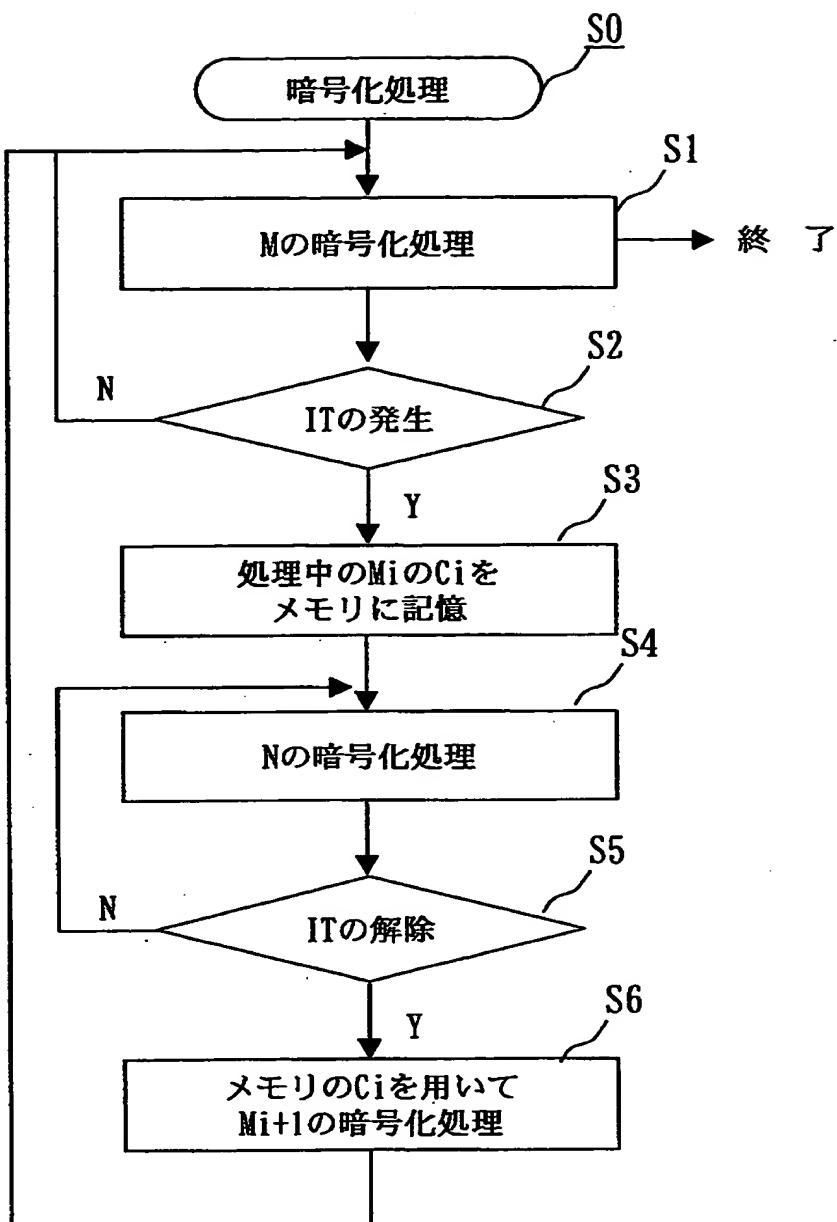
【図1】



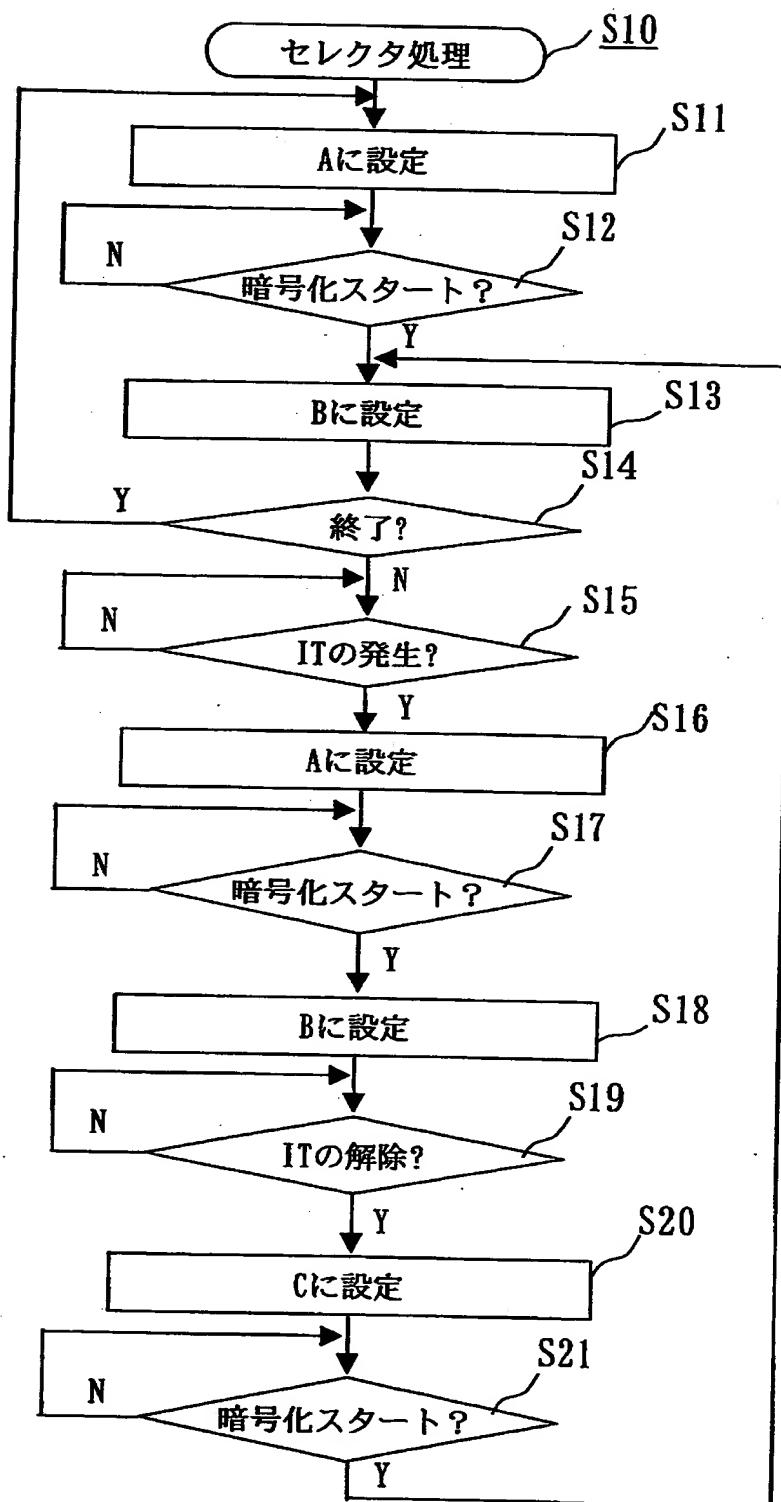
【図2】



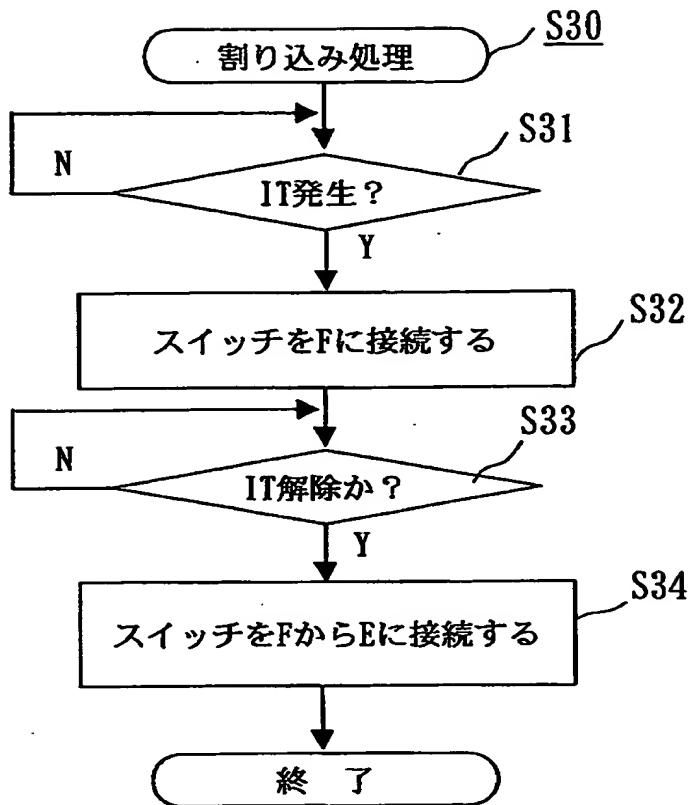
【図3】



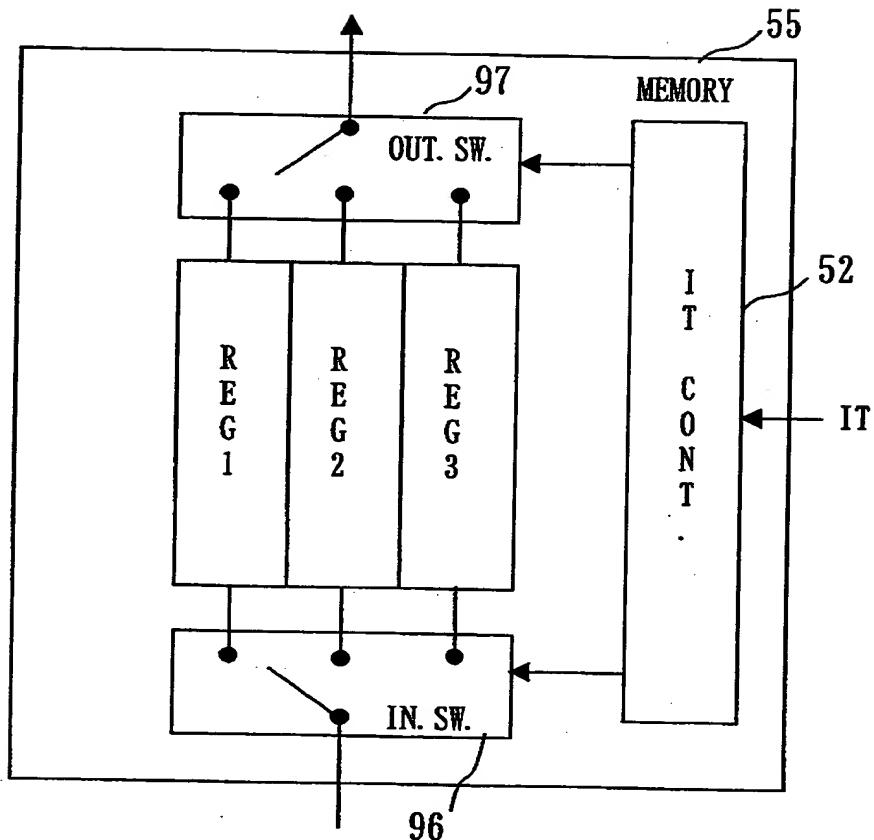
【図4】



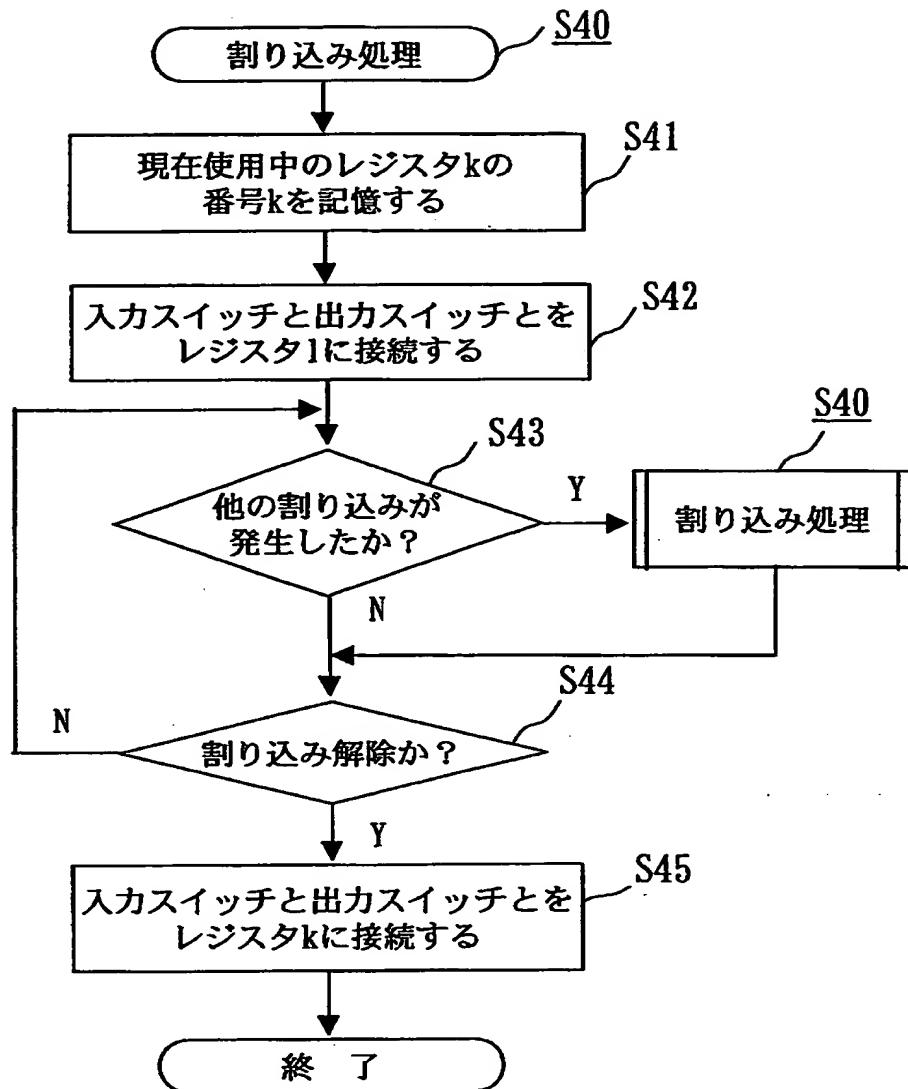
【図5】



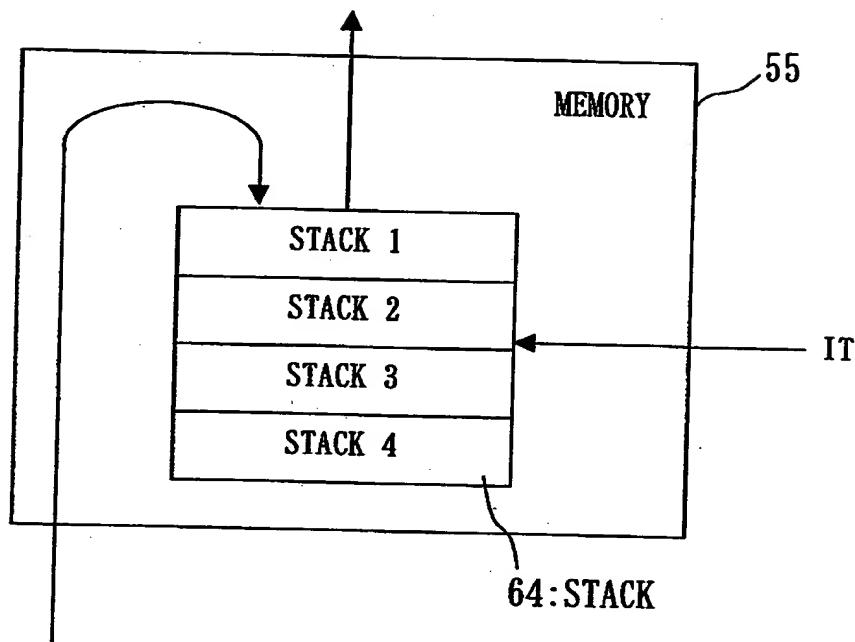
【図6】



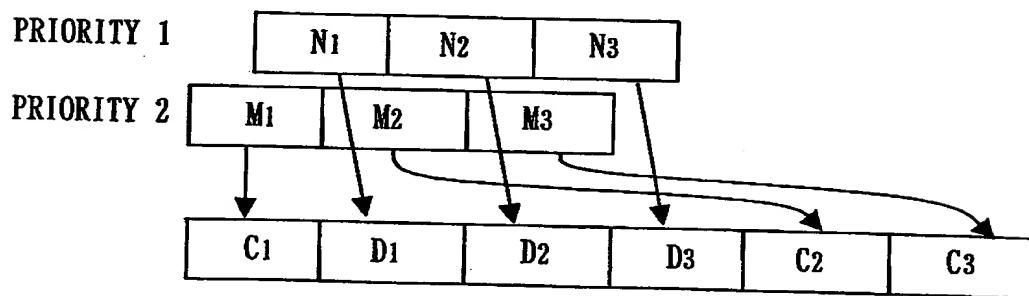
【図7】



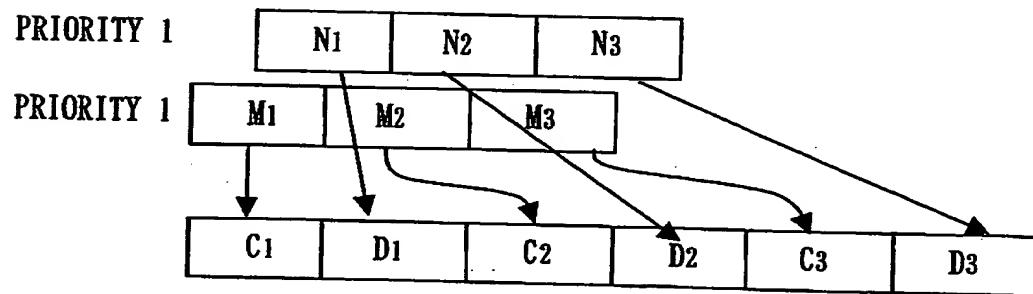
【図8】



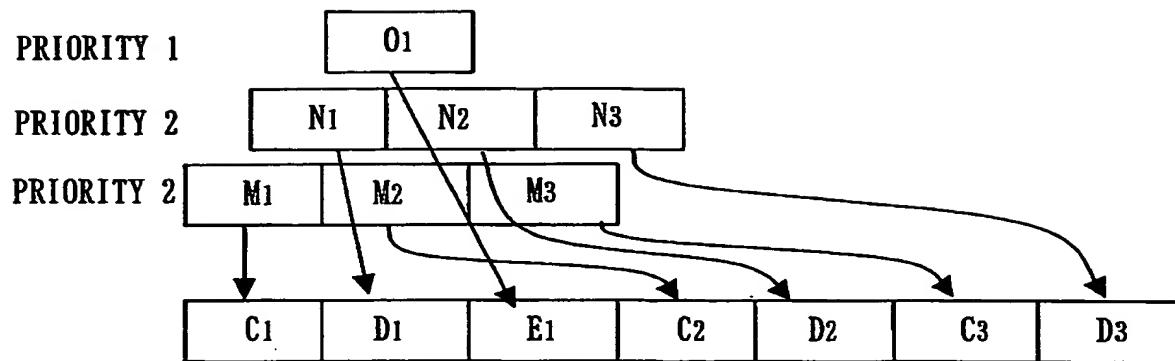
【図9】



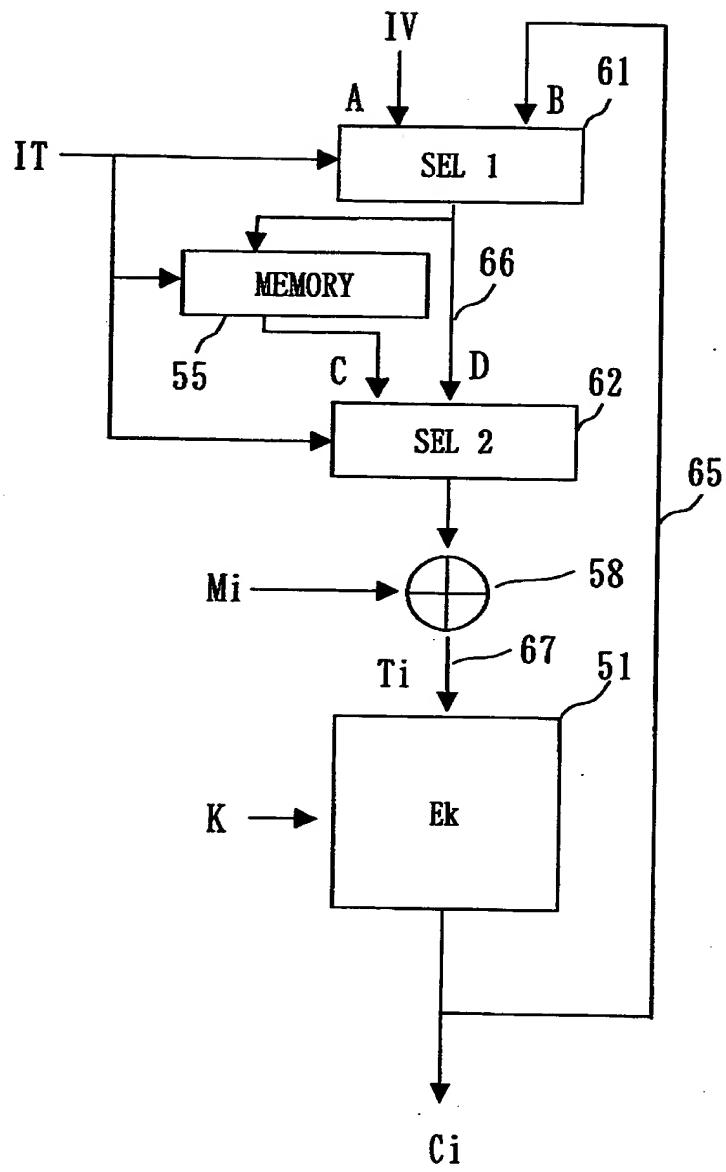
【図10】



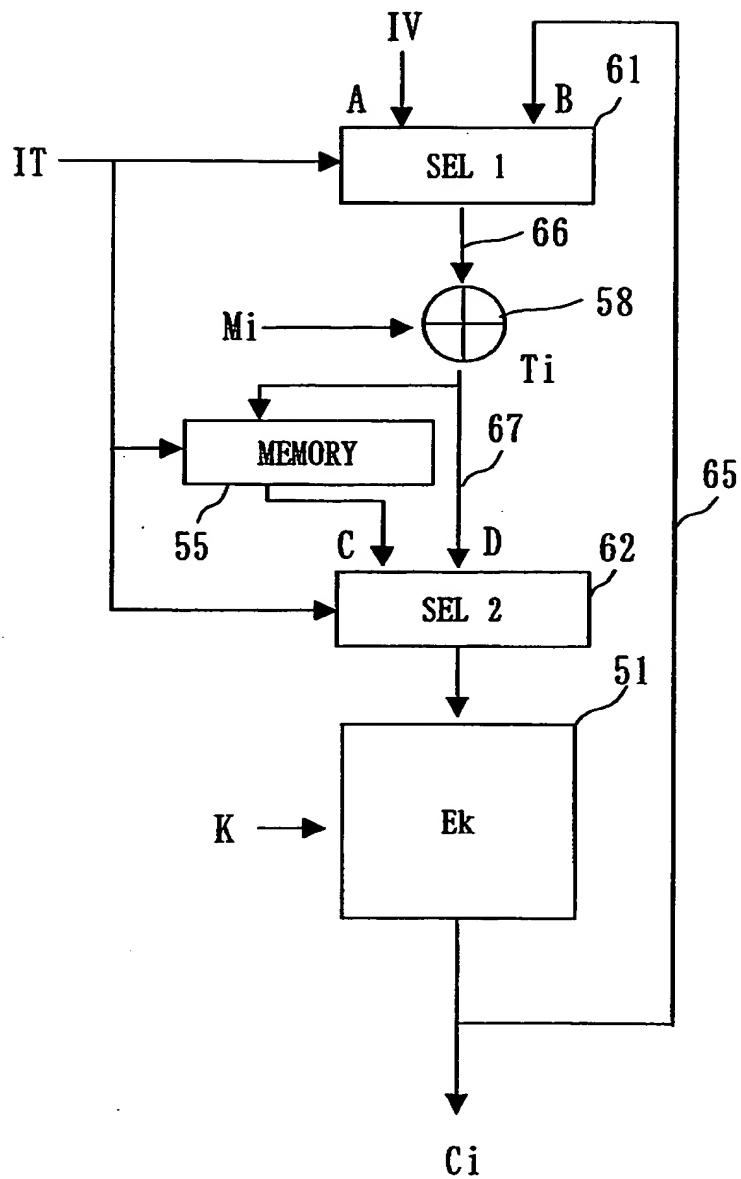
【図11】



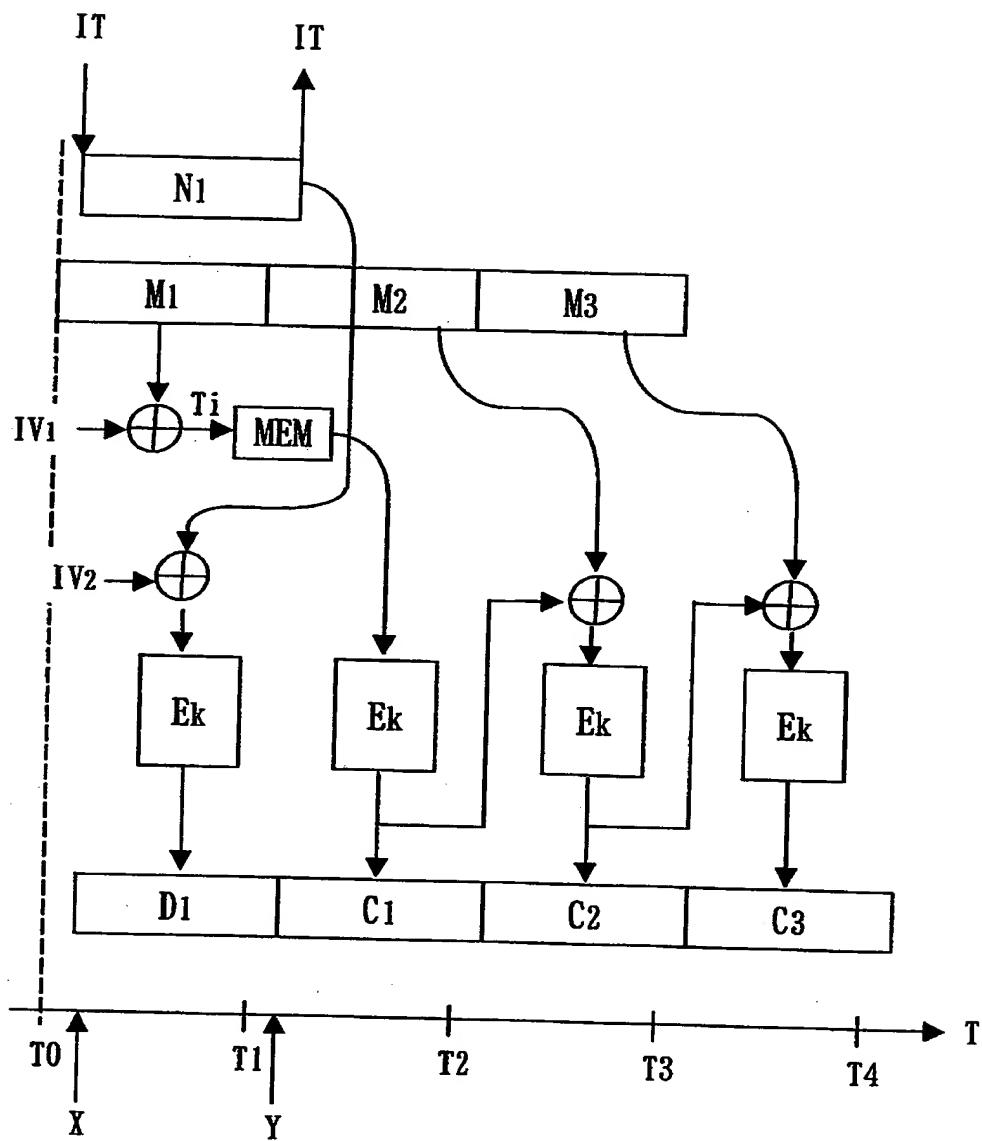
【図12】



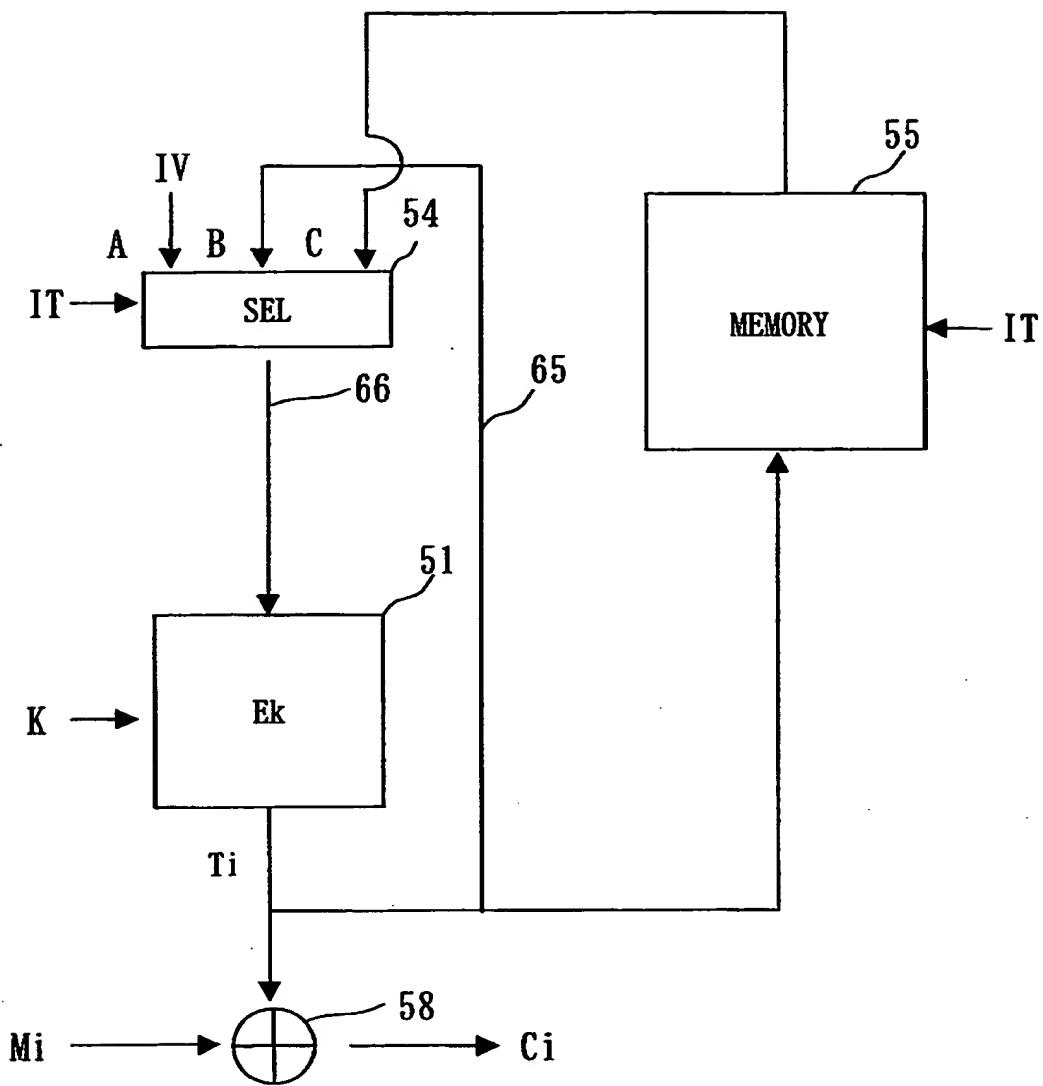
【図13】



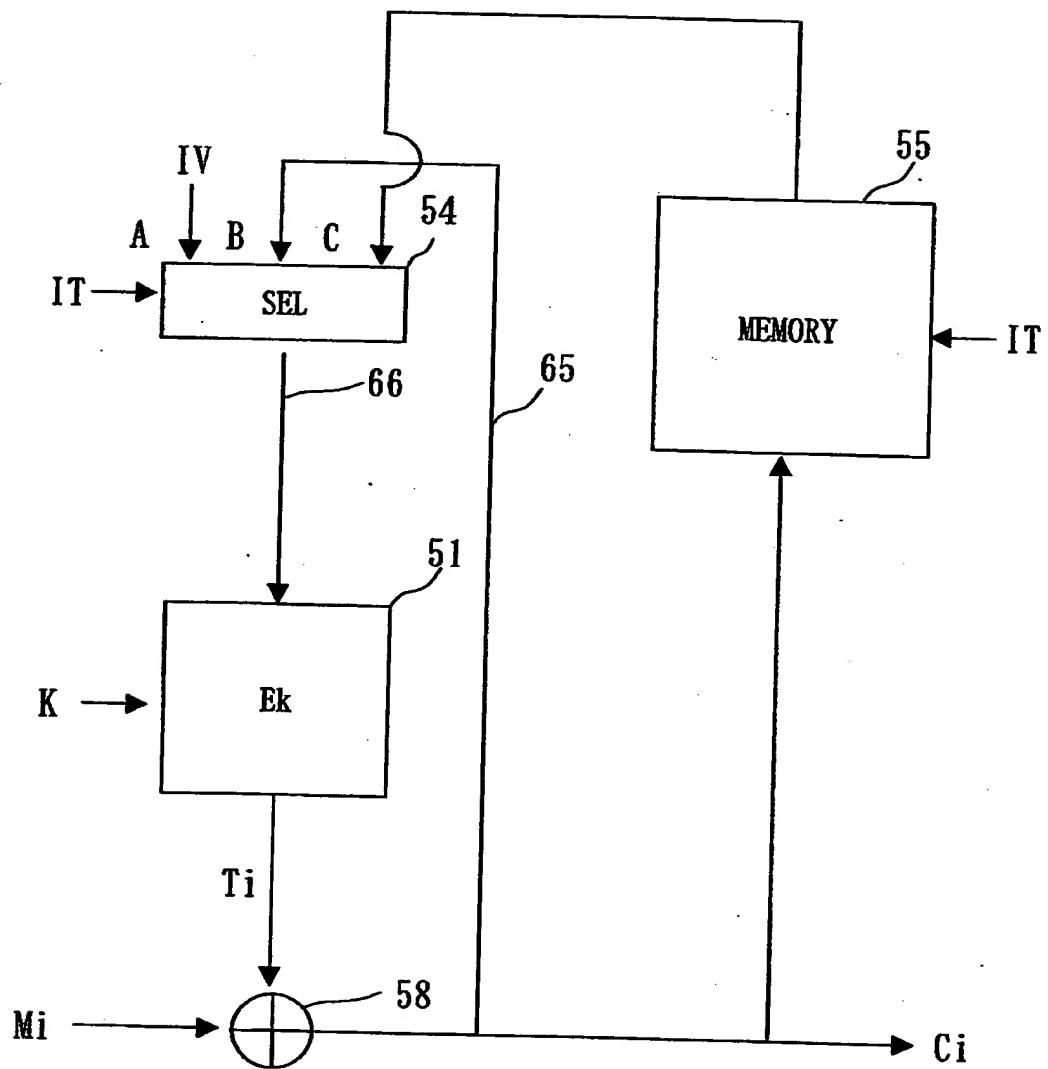
【図14】



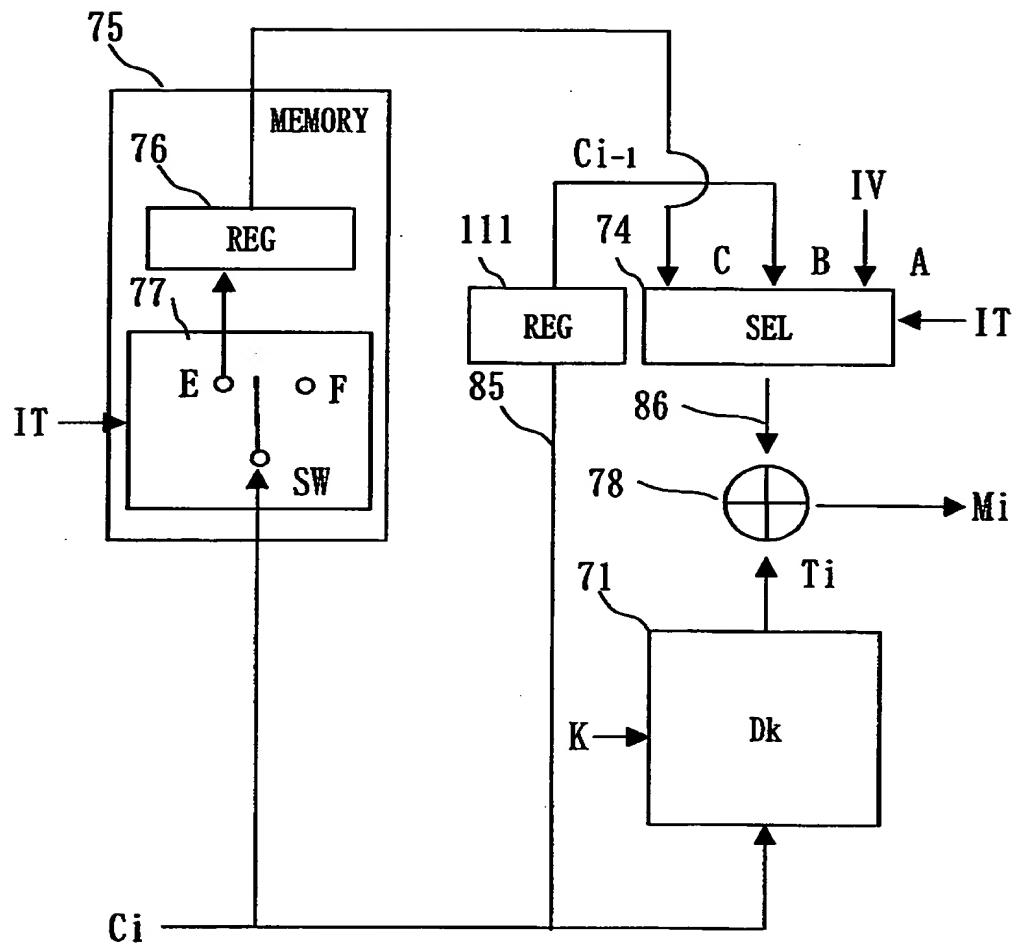
【図15】



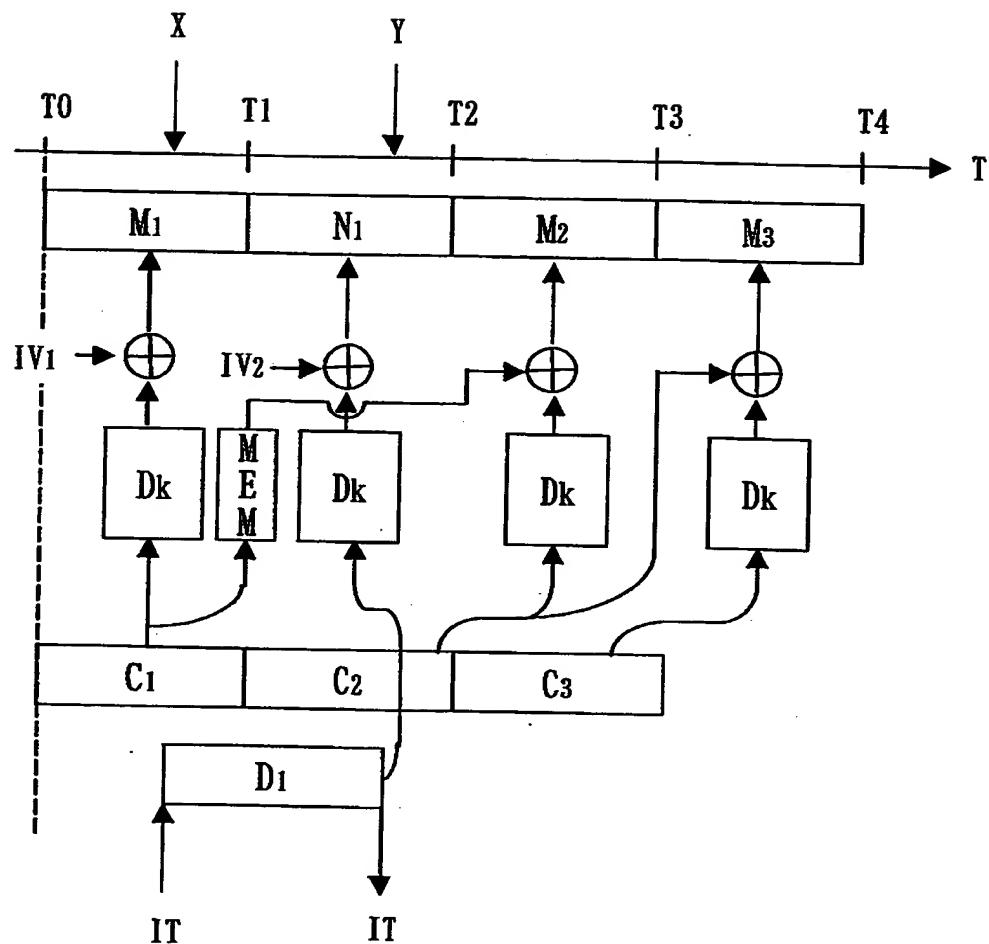
【図16】



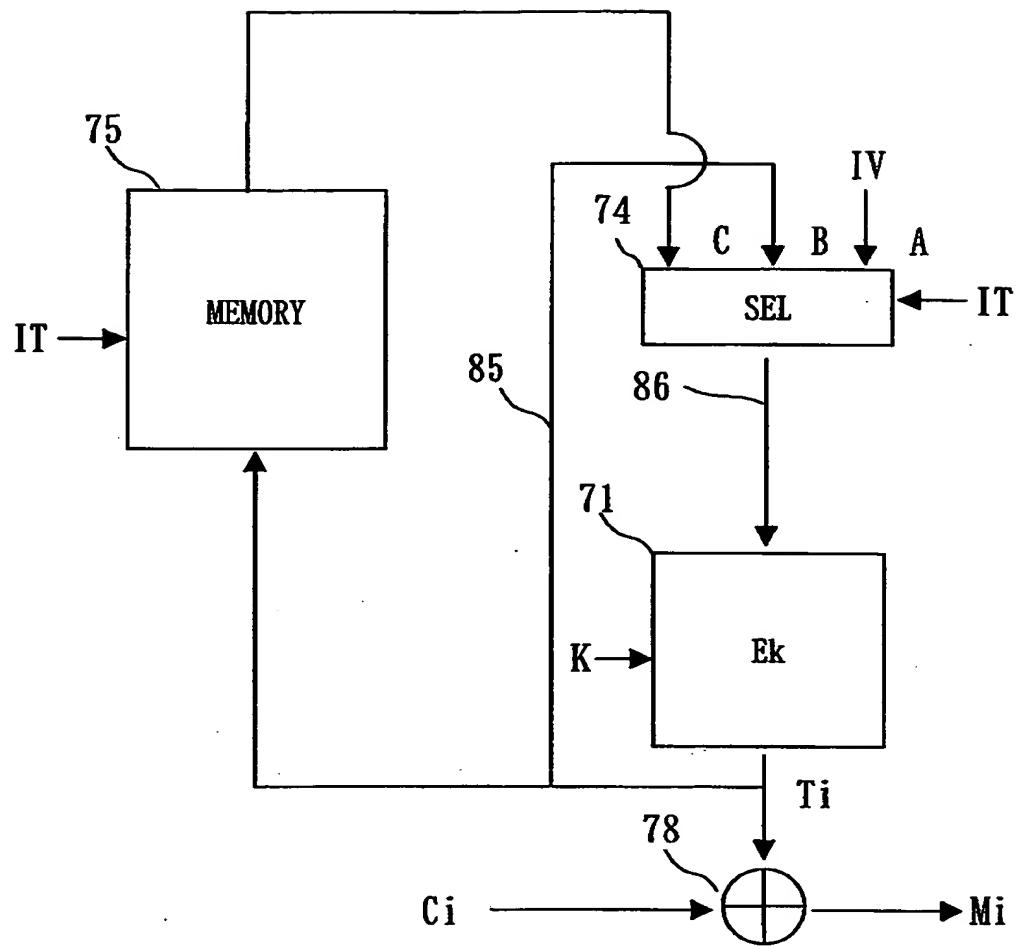
【図17】



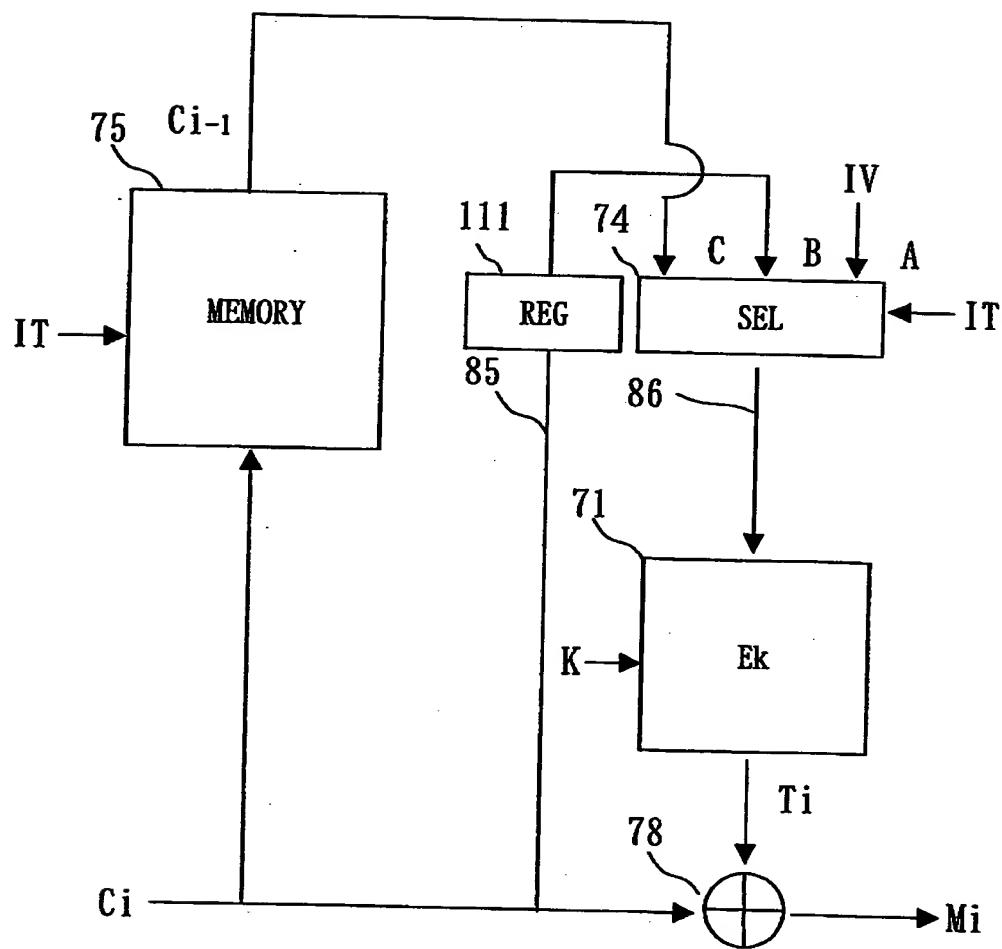
【図18】



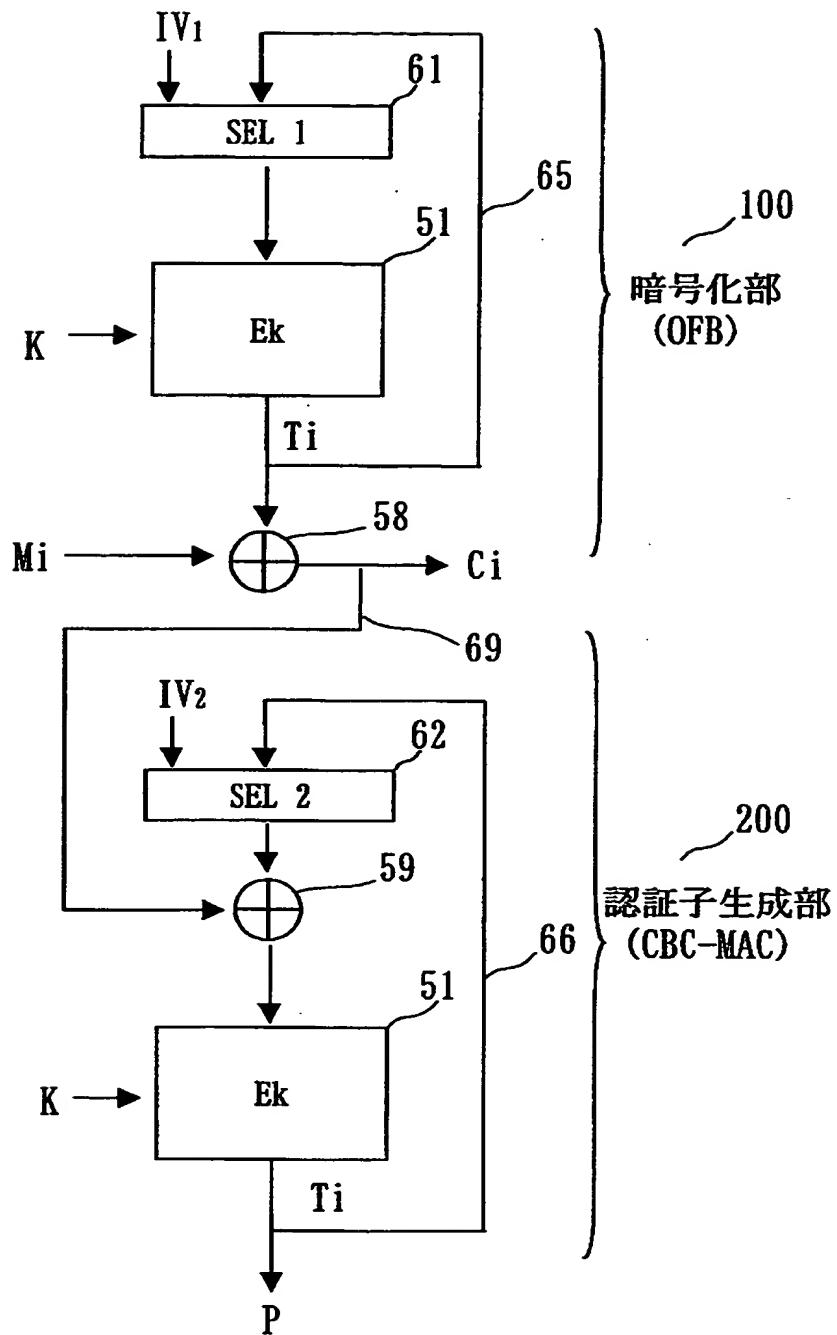
【図19】



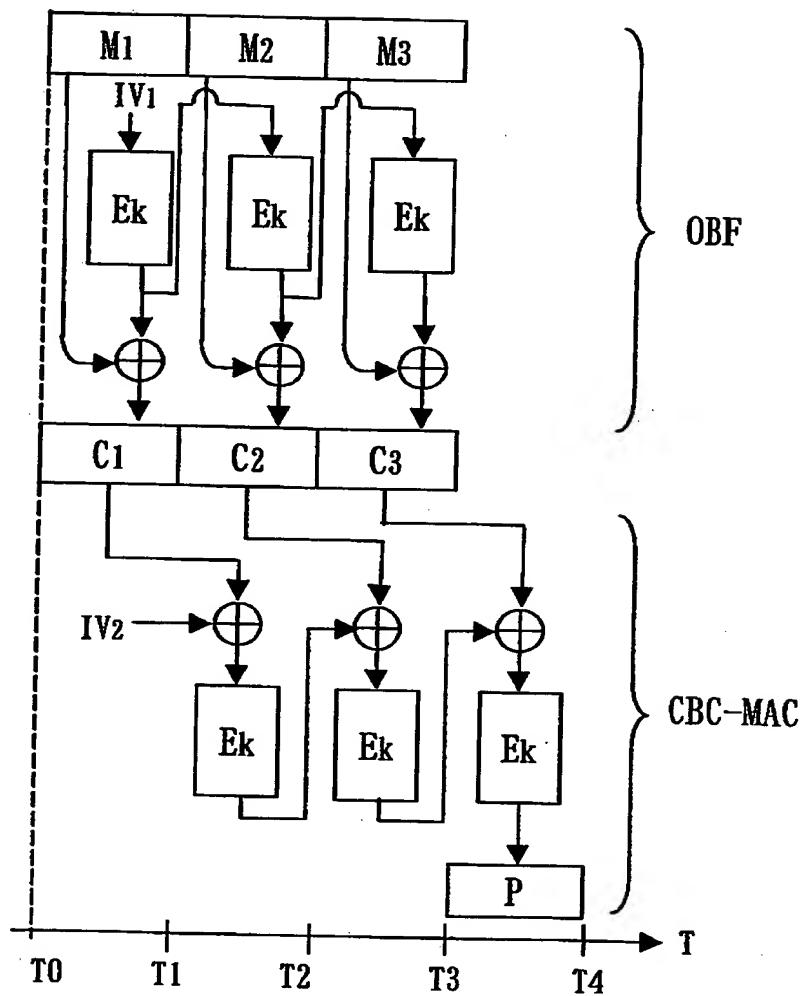
【図20】



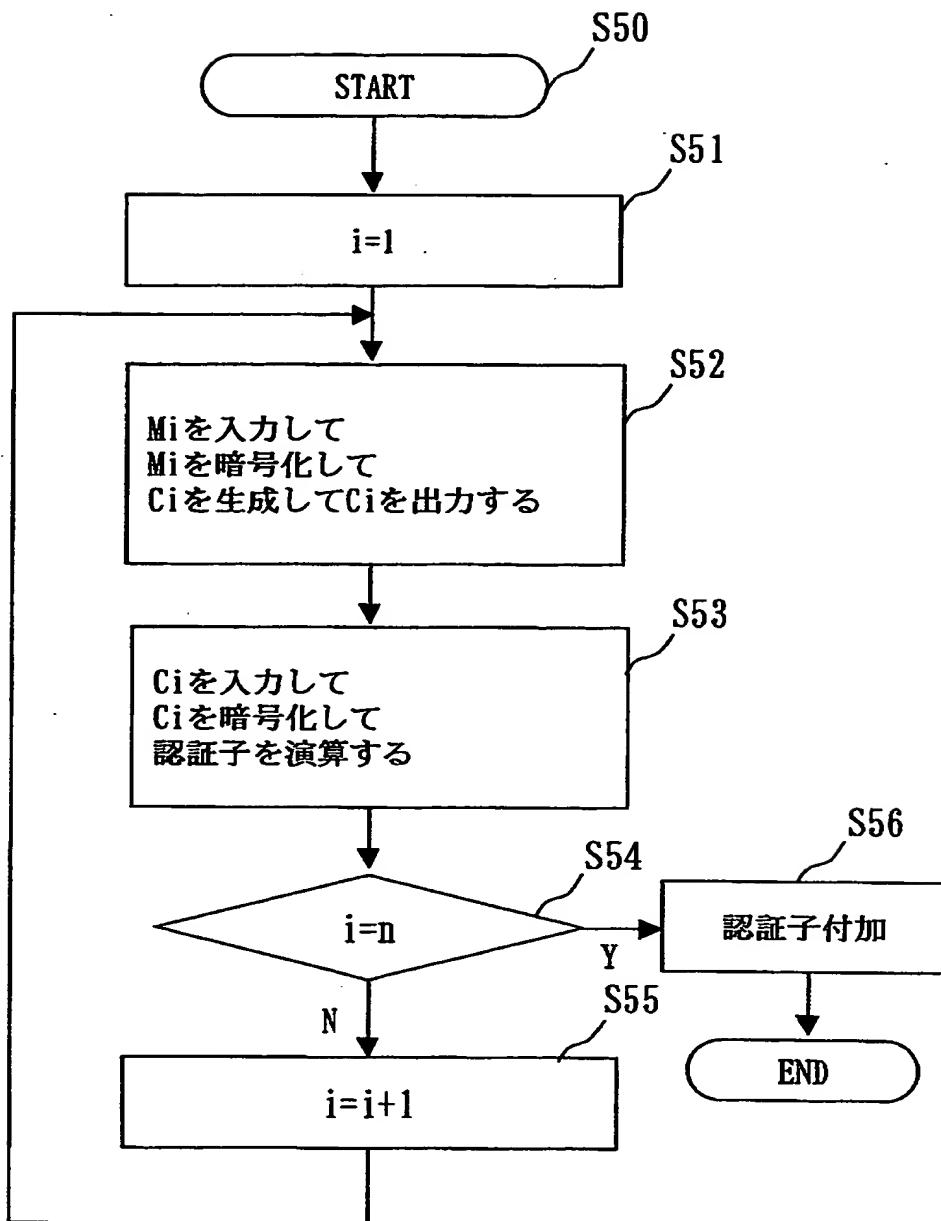
【図21】



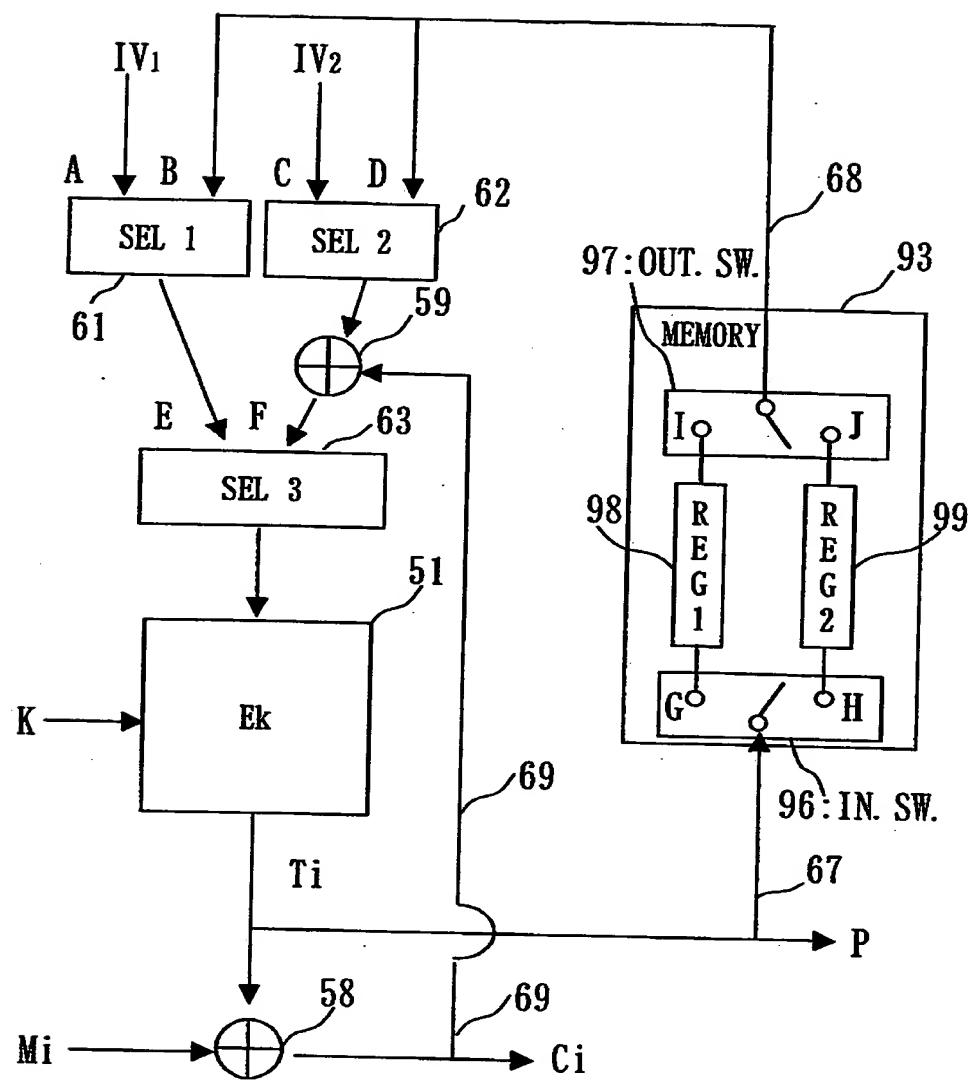
【図22】



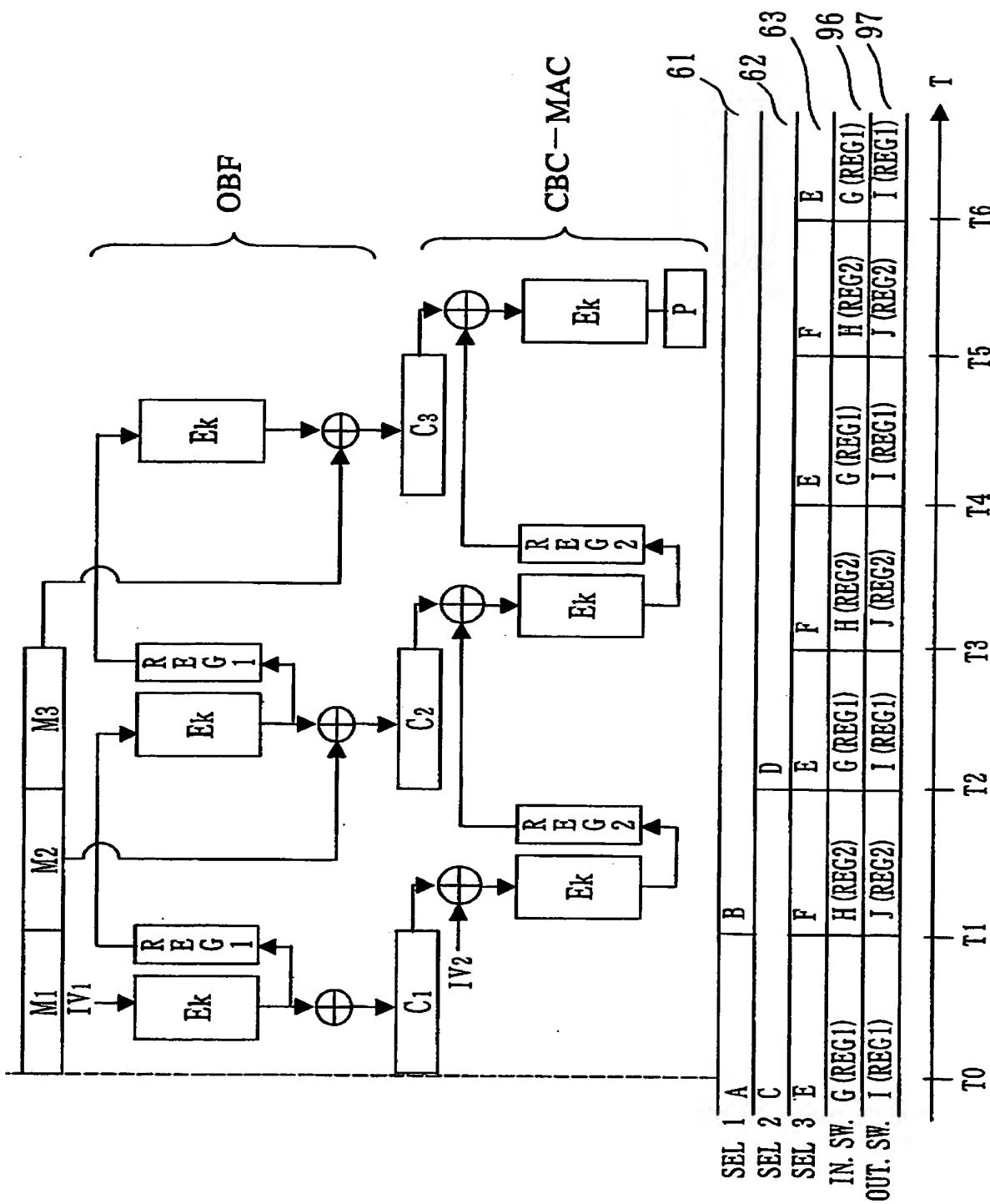
【図23】



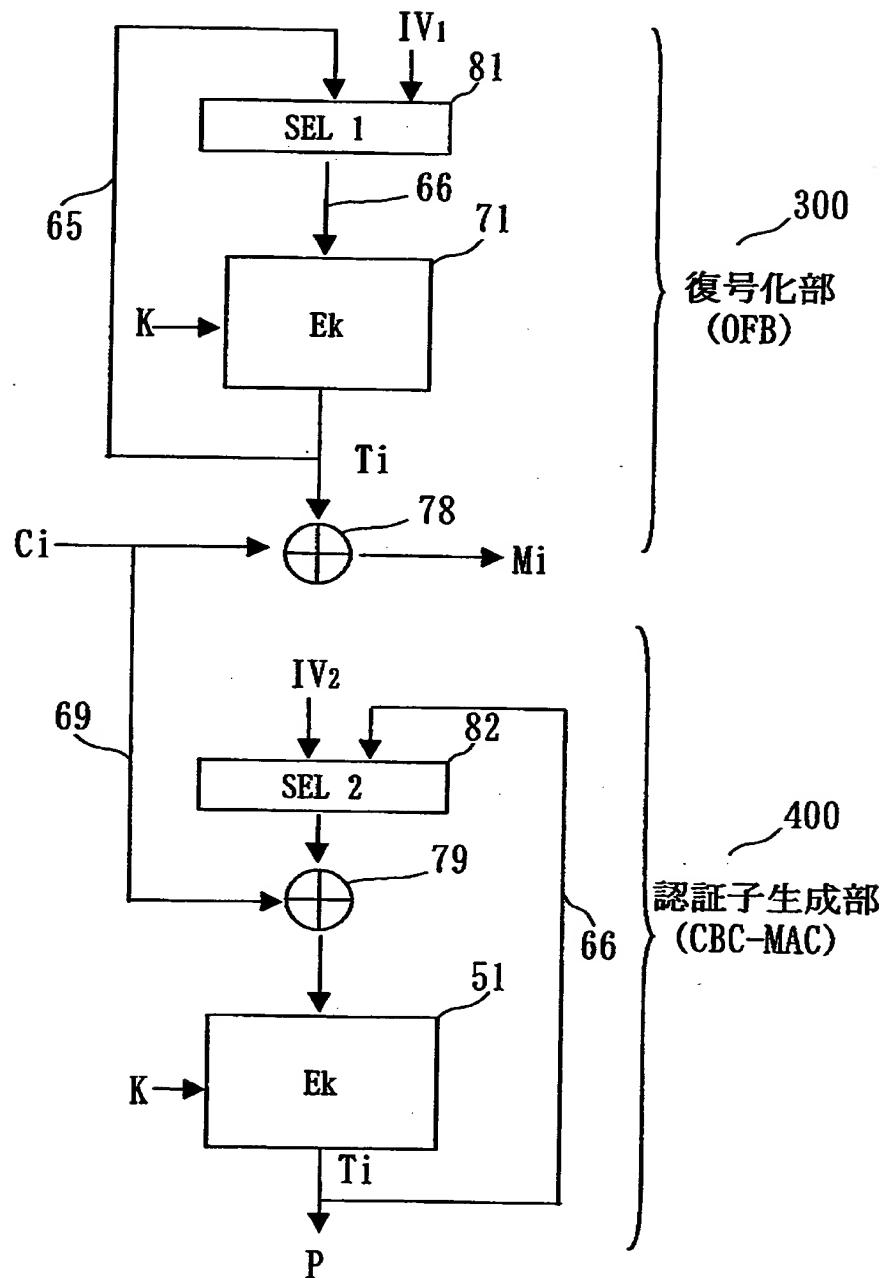
【図24】



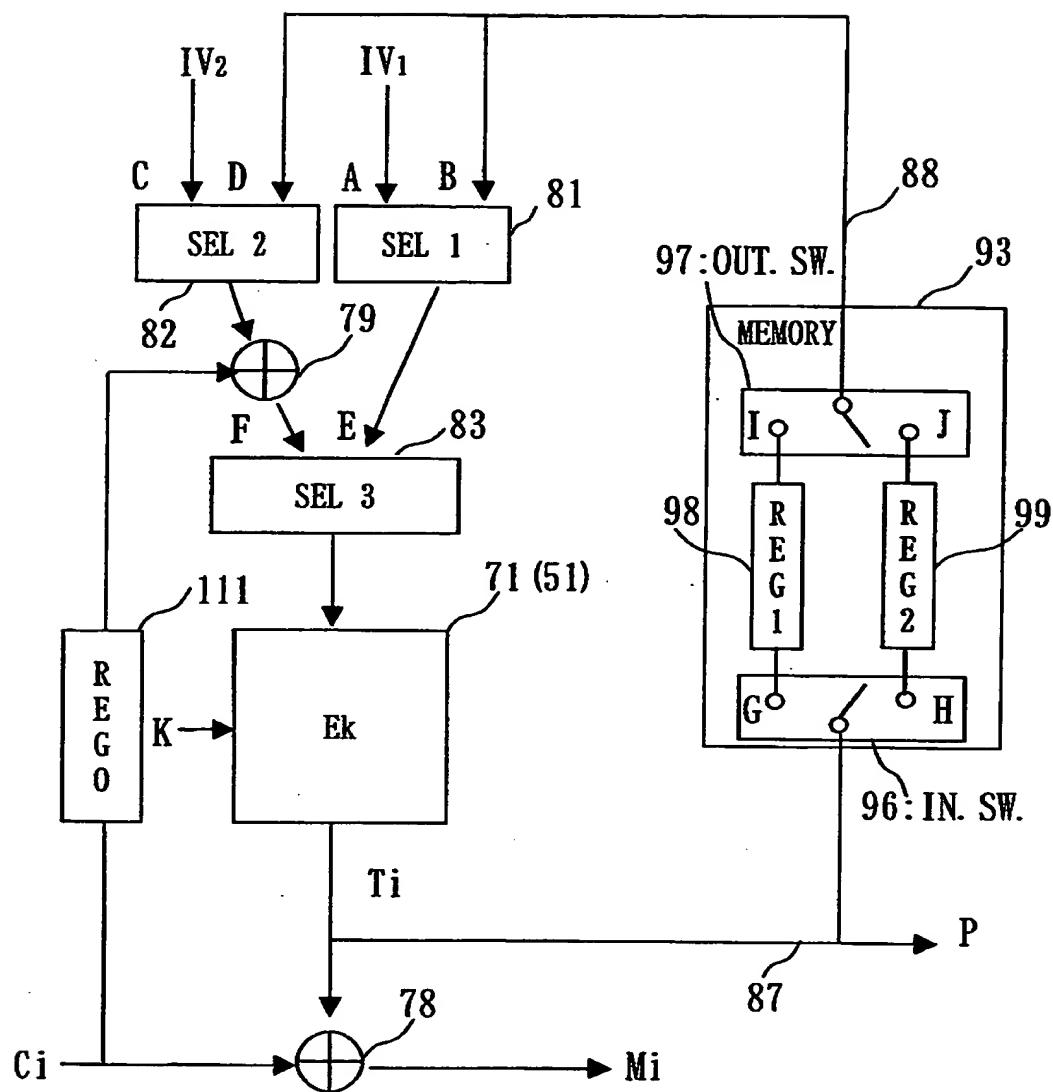
【図25】



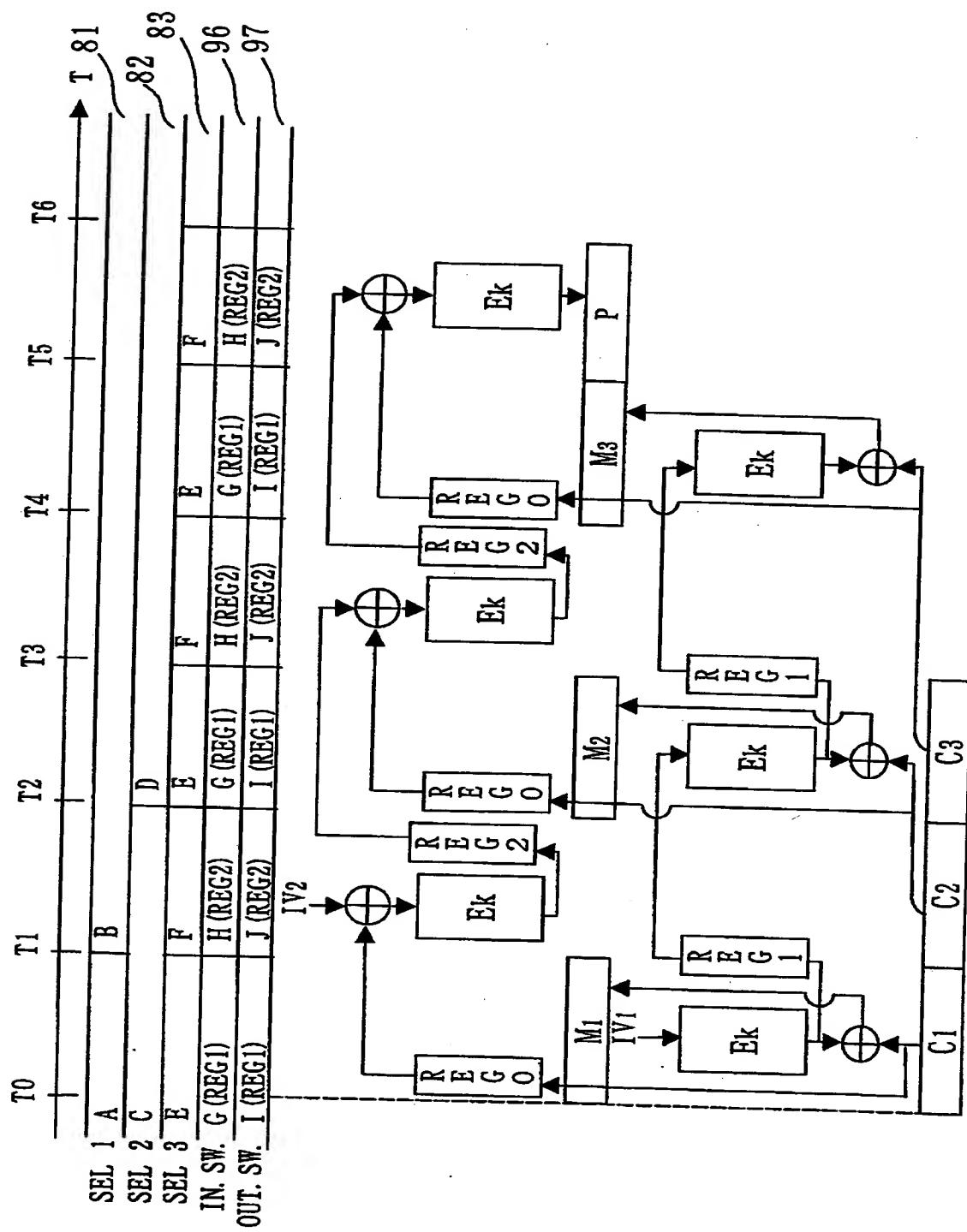
【図26】



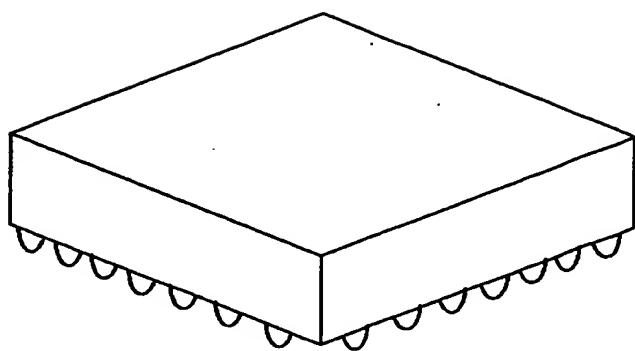
【図27】



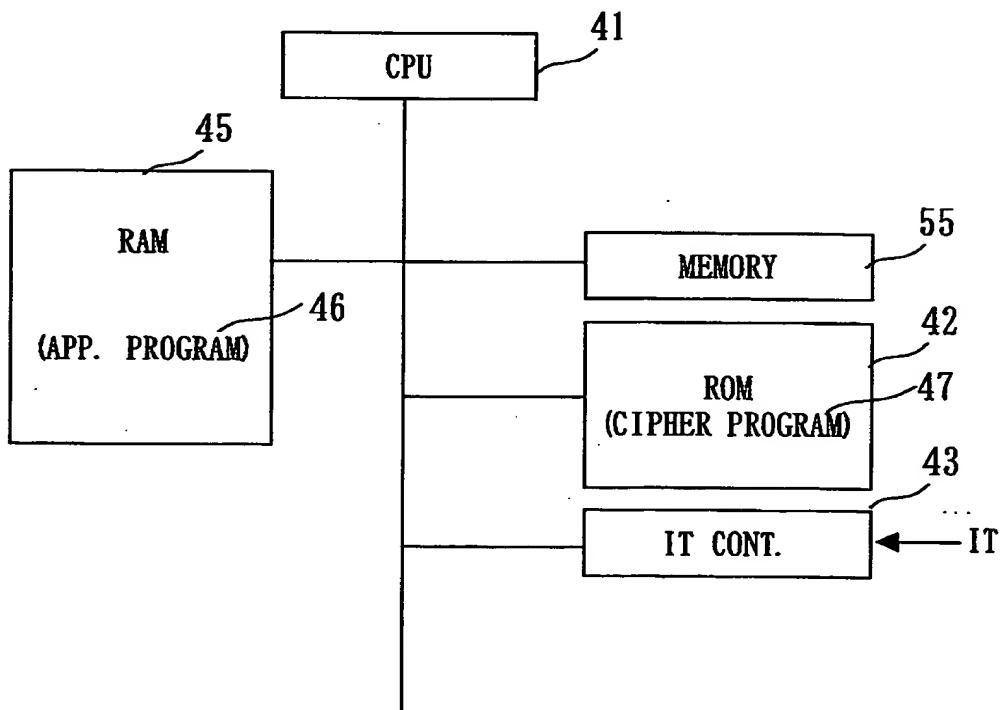
【図28】



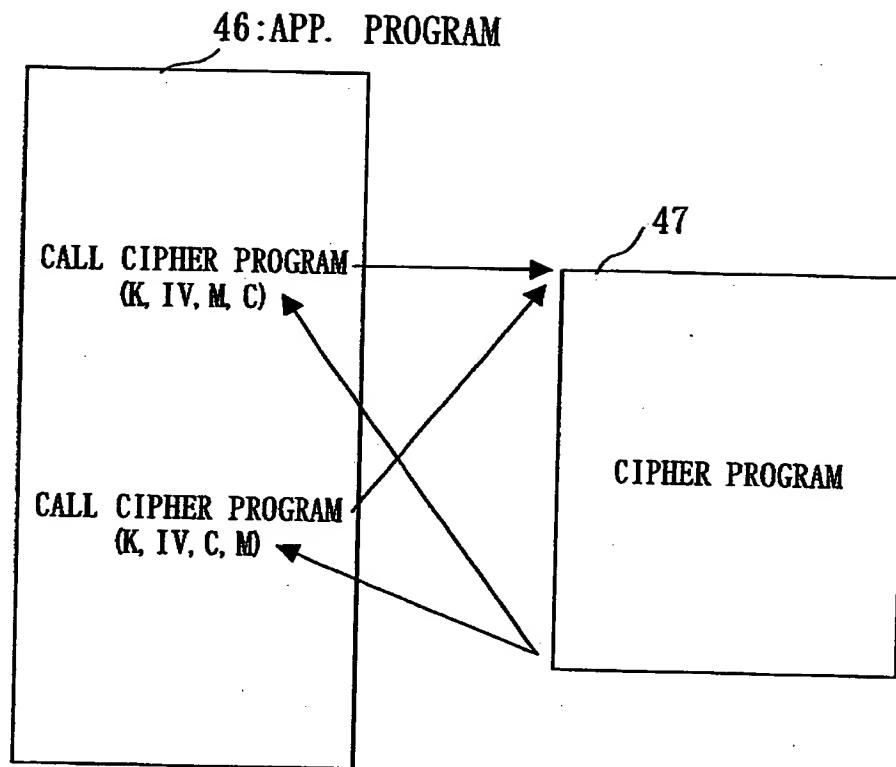
【図29】



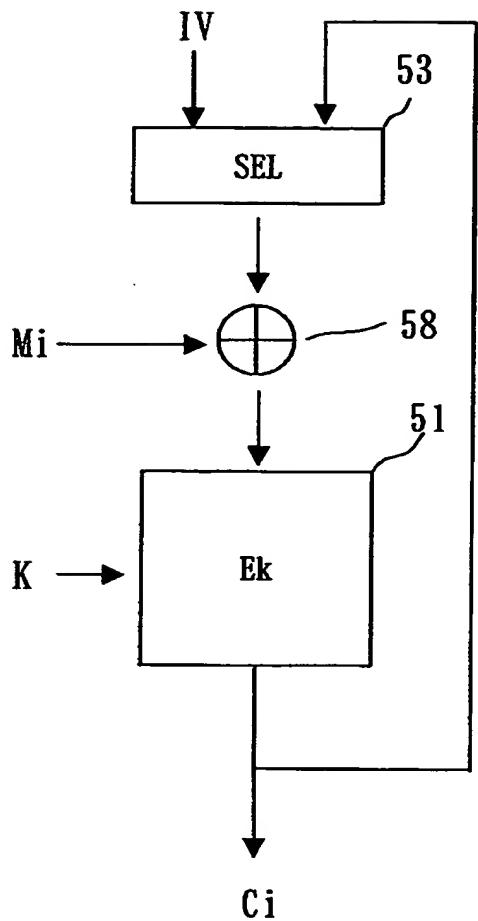
【図30】



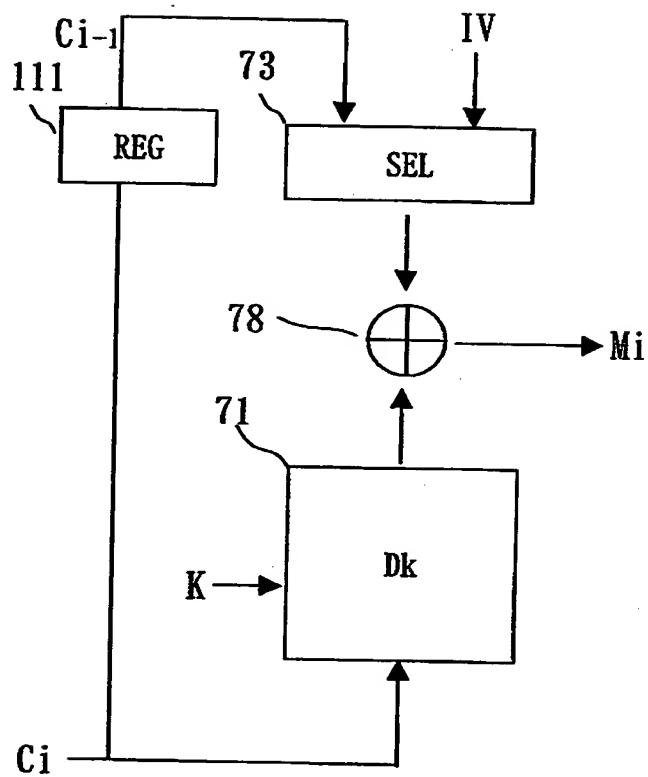
【図31】



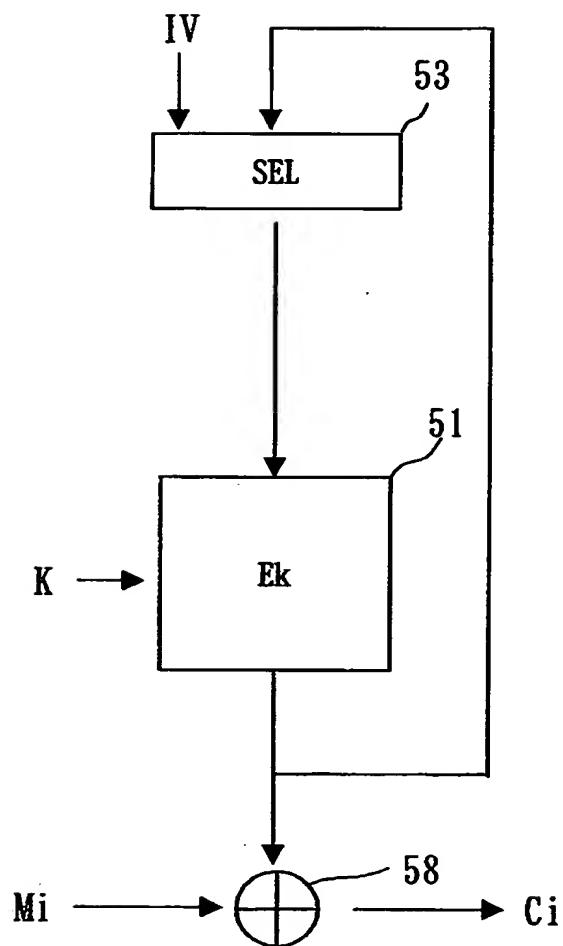
【図32】



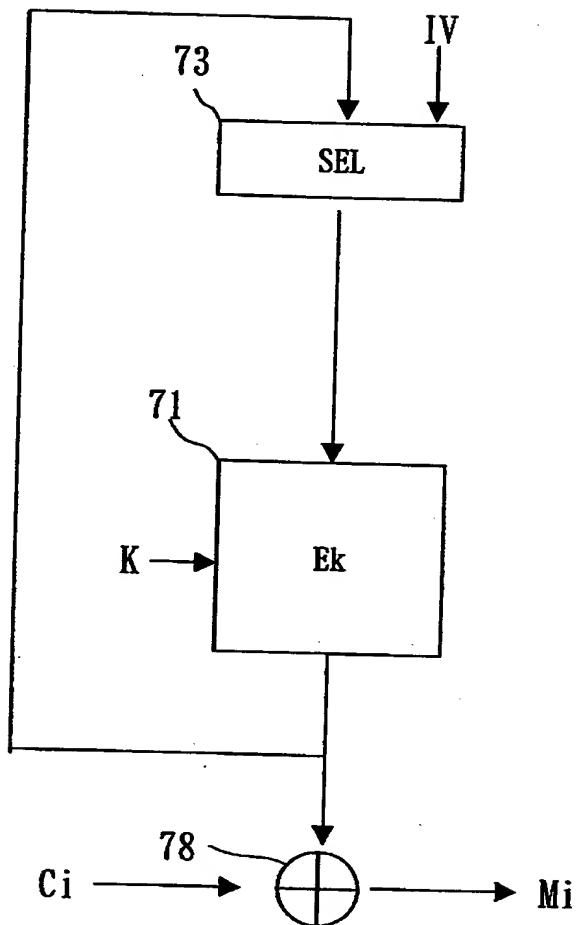
【図33】



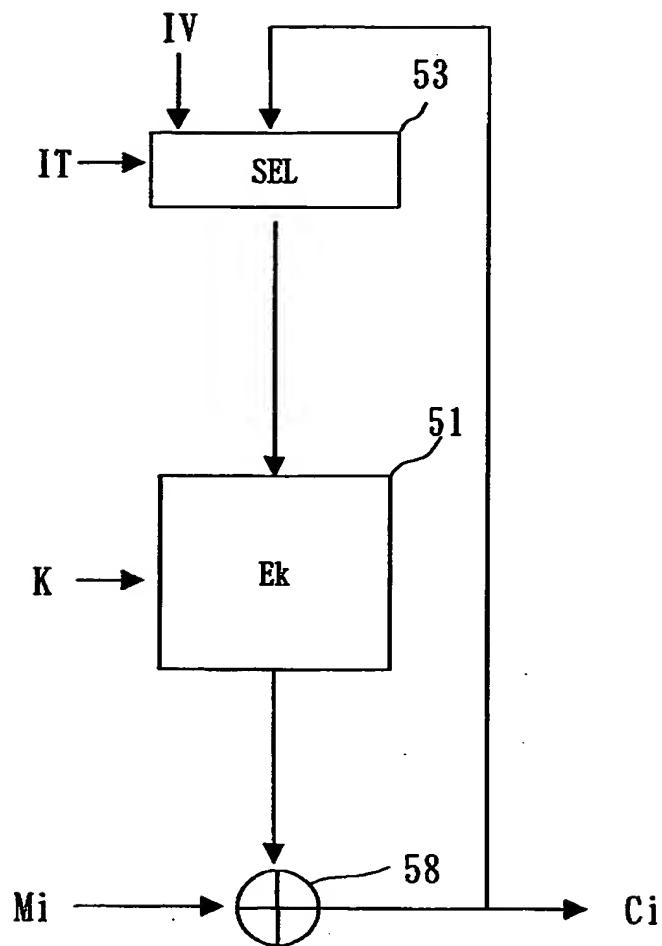
【図34】



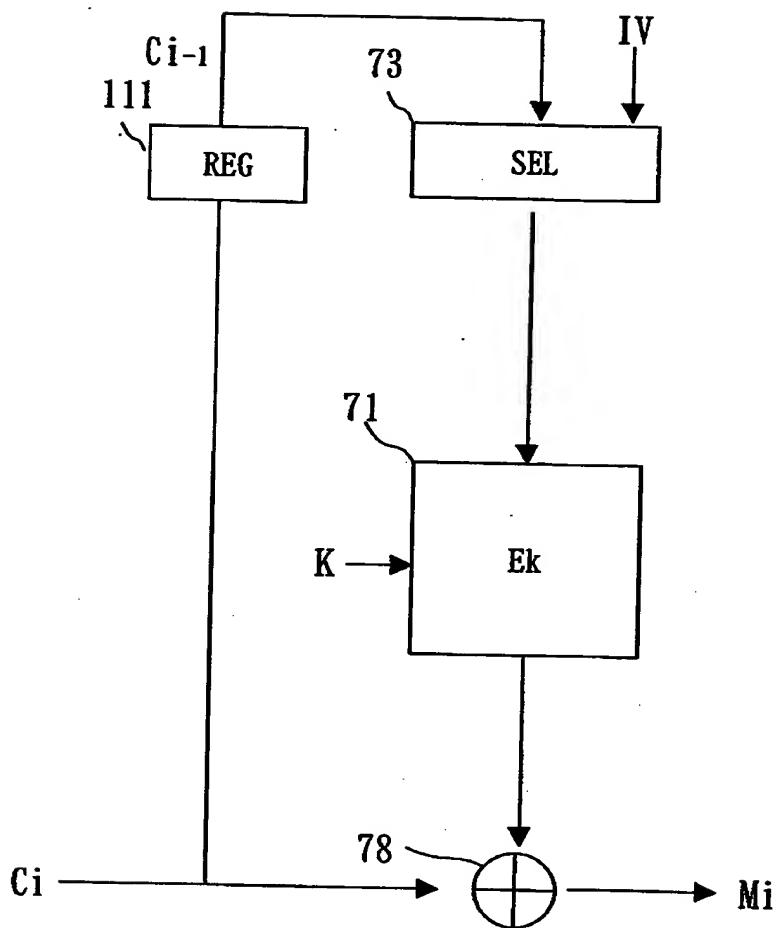
【図35】



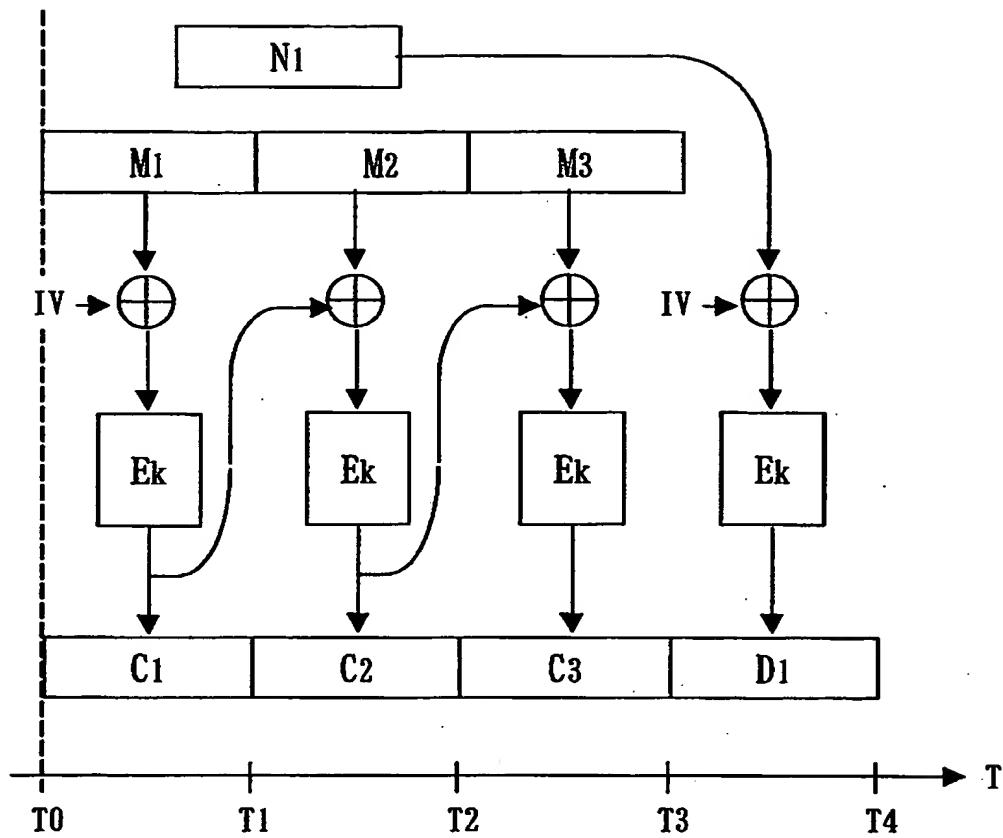
【図36】



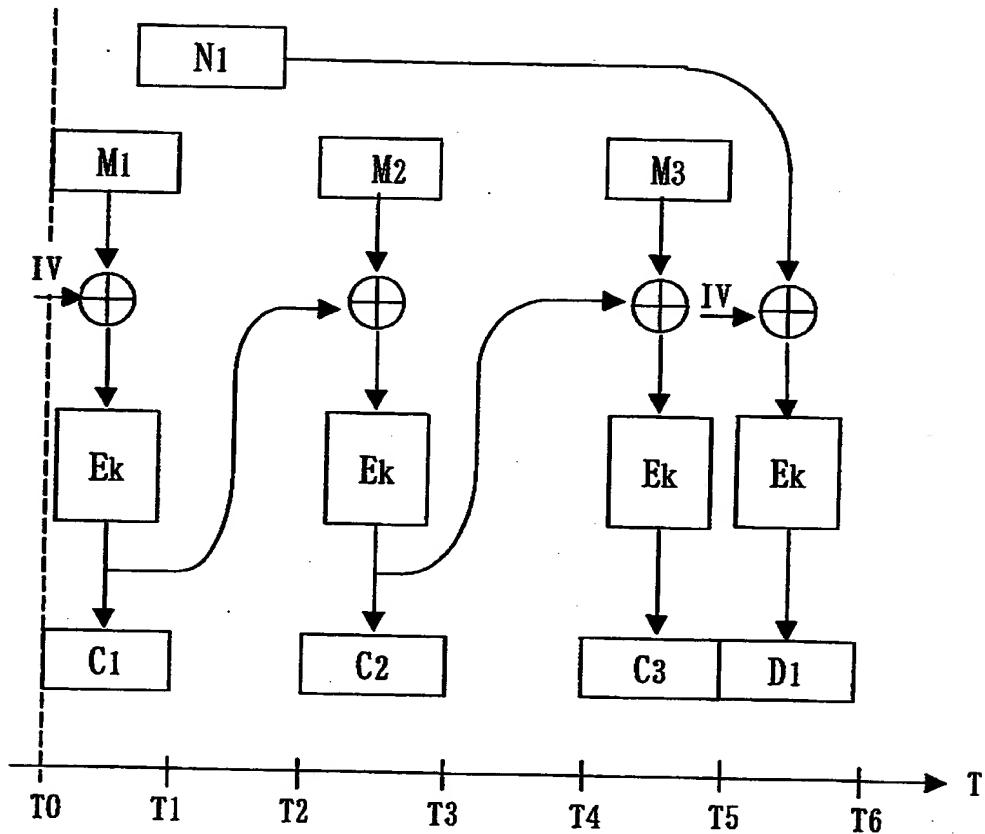
【図37】



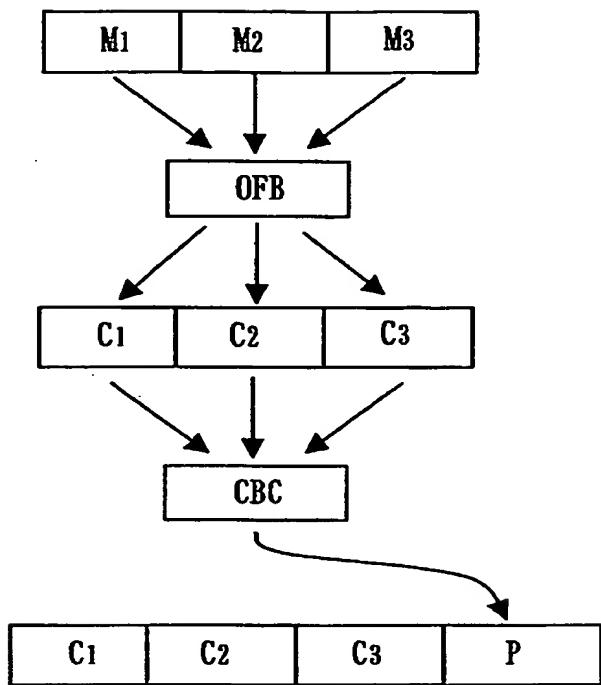
【図38】



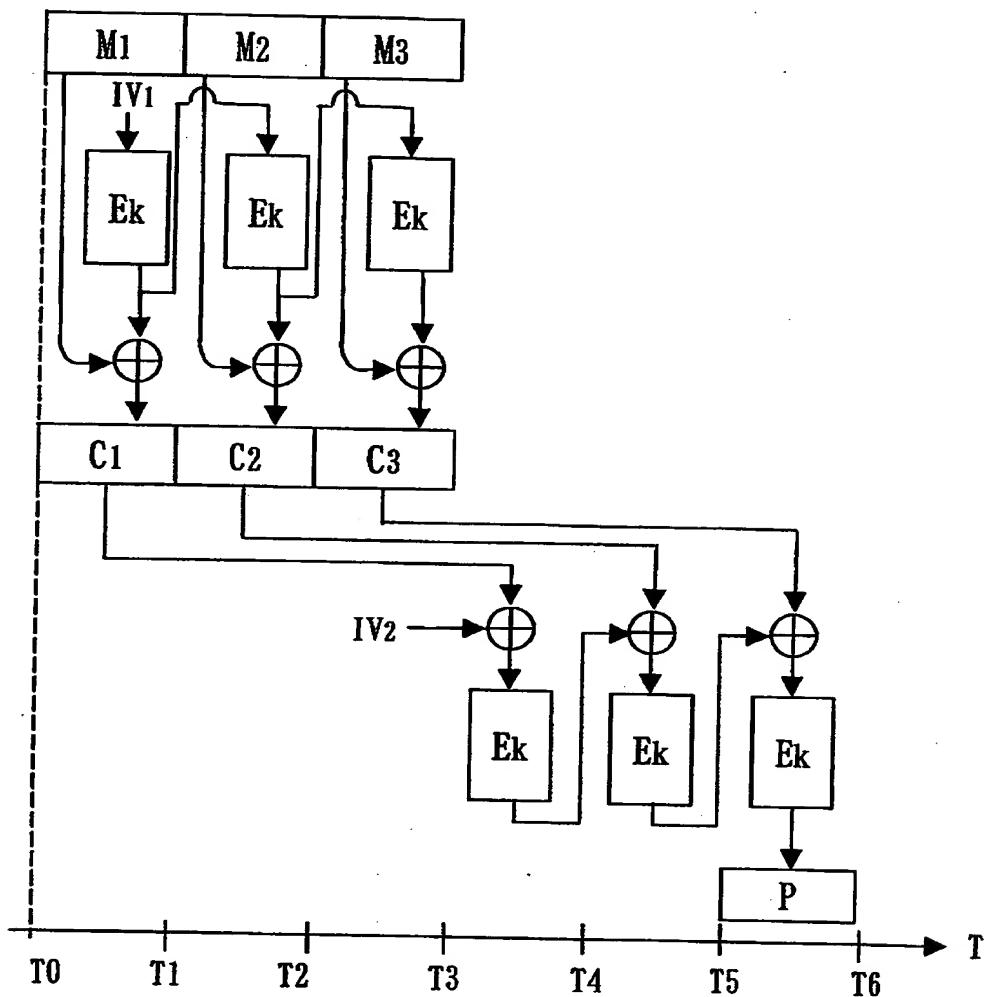
【図39】



【図40】



【図41】



【書類名】 要約書

【要約】

【課題】 暗号化の最中に他のデータの暗号化を行いたい。

【解決手段】 暗号鍵Kを用いた暗号化モジュール51からセレクタ54にフィードバックするフィードバックライン65に対して並列に設けられたメモリ55を配置する。平文ブロックデータ M_i を処理中に他のデータの平文ブロックデータ N_i を処理する割り込みITが発生した場合には、割り込みITが発生したときの暗号文ブロックデータ C_i をレジスタ56に記憶させ、平文ブロックデータ N_i の処理が終了した時点でメモリ55に記憶した暗号文ブロックデータ C_i をセレクタ54に選択されることにより平文ブロックデータ M_{i+1} の処理を開始する。

【選択図】 図1

特2000-05161

出願人履歴情報

識別番号 [000006013]

1. 変更年月日 1990年 8月24日

[変更理由] 新規登録

住 所 東京都千代田区丸の内2丁目2番3号

氏 名 三菱電機株式会社